CITY AUDITOR'S OFFICE

Selected Application Controls over the City's TotalHR® System

December 27, 2010 **AUDIT REPORT NO. 1104**

CITY COUNCIL
Mayor W.J. "Jim" Lane
Lisa Borowsky
Wayne Ecton
Vice Mayor Suzanne Klapp
Robert Littlefield
Ron McCullagh
Marg Nelssen

December 27, 2010

Honorable Mayor and Members of the City Council:

Enclosed is the audit report, *Selected Application Controls over the City's TotalHR® System.* This system maintains City employee information related to assignment, pay and benefits, and it processes payroll.

The audit assessed effectiveness of selected TotalHR® application controls, specifically including those for system access, change management, and security management. Generally, there are sufficient procedures, reviews and reconciliations to identify and manage potential risks to the TotalHR® system. In addition, technology staff have a business continuity plan for restoring the system in the event of an unexpected interruption. However, some improvements can be made to system access rights, change management processes, and system security.

We would like to thank the staff from the Finance & Accounting, Human Resources, 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, Assistant City Auditor
Lee Pettit, Sr. Auditor
Erika Keel, Auditor

TABLE OF CONTENTS

Executive Summary 1

Background 2

Objectives, Scope, and Methodology 4

Findings and Analysis 5

1. A few users have more system access than needed and authorizations can be improved. 5
2. Standardizing TotalHR® change management requirements would provide better assurance that changes have been properly authorized and tested. 7
3. Security improvements can be made to better protect TotalHR® 7

Action Plan 9

EXECUTIVE SUMMARY

An audit of Information Technology Controls of selected City information systems was included on the Council-approved fiscal year 2010/11 audit plan. For this audit, the City's TotalHR® application, which maintains employee information, including assignment, pay and benefits, and processes payroll, was selected. The audit objective was to assess the effectiveness of TotalHR® application-level controls, focusing on system access, change management, and security management.

The TotalHR® application, which the City implemented about fifteen years ago, serves both human resources (HR) and payroll functions. The HR division is responsible for employment and benefit data, and the Payroll department within Finance & Accounting is responsible for payroll functions and data. TotalHR® is supported by the Information Technology Division, primarily through the services of the Financial Services Technology Director, a systems integrator and a technology specialist assigned to the Finance & Accounting division.

Generally, there are sufficient procedures, reviews and reconciliations to identify and manage potential risks to the TotalHR® system. In addition, technology staff have a business continuity plan for restoring the system in the event of an unexpected interruption. However, this established application is supported by experienced staff so the processes and documentation that have been put in place are less formal. Therefore some improvements can be made to system access rights, change management processes, and system security.

BACKGROUND

The City of Scottsdale selected and implemented TotalHR® for the City's human resources and payroll software in 1994. TotalHR® is used to maintain employment and benefit information and process payroll for about 2,600 full and part-time employees annually, or about 66,000 employee payments in FY 2010/11, as shown in Table 1.

Table 1. Number of Employee Payments by Fiscal Year

Fiscal Year	Number of Employee Payments (rounded)
2010/11 est.	66,000
2009/10	72,000
2008/09	77,000
2007/08	76,000
2006/07	74,000

SOURCE: Auditor analysis of City of Scottsdale Payroll Statistics for fiscal years 2006/07- first quarter 2010/11.

The Payroll department within Finance & Accounting enters pay and tax information for new and existing employees, while the Human Resources division enters new employee benefit information, CDL and I-9 verification. Since June 2010, existing employees directly enter their own annual benefit selections through Scottsdale's Employee Self-Service portal.

The TotalHR® application, which resides on the City's network, is primarily maintained by Information Technology (IT) staff assigned to the Finance & Accounting Division. This staffing includes a systems integrator and a technology specialist who report to the Financial Services Technology Director. Assistance is also available from two Human Resources (HR) technical support staff who primarily support other HR programs such as the online application system and document management system.

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 TotalHR®. 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 TotalHR® application-level general controls, focusing on system access, change management, 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.

OBJECTIVES, SCOPE, AND METHODOLOGY

An audit of Information Technology (IT) Controls was included on the Council-approved fiscal year 2010/11 audit plan; the City's TotalHR® 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 TotalHR® system's application-level general controls over system access, change management, and security management.

To gain an understanding of TotalHR® system's application-level general controls, we reviewed the written pay period procedures and production checklist. We also interviewed key members of the Payroll, Human Resources, and IT staff who use or support the system regarding their processes, reviews and reconciliations.

In designing tests of controls, we used the Information Systems Audit and Control Association's (ISACA) *IT Audit and Assurance Guidelines* G14, G37, G38, and G40 related to change management, system access, and system security. We also used the U.S. Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual (FISCAM)* 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 TotalHR® user. This included a review for appropriate segregation of duties among the authorized users.

Change Management
Verified that the TotalHR® test environment matched the production environment on the test date of November 17, 2010.

Reviewed TotalHR® change management processes and the listing of TotalHR® system changes. We also examined documentation supporting a sample of the most recent system changes.

Security Management
Reviewed system security parameters, such as password length, concurrent sessions, automatic timeouts, and number of user login attempts allowed. In addition, we inquired about system security training provided to TotalHR® users and performed limited testing on the security levels set in the City's Document Management system which retains the supporting documentation for TotalHR® data and transactions.

In addition to performing these procedures for our primary objectives, we reviewed the business continuity plan for TotalHR®.

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 November through December 2010, with Joyce Gilbride, Lee Pettit, and Erika Keel conducting the work.

FINDINGS AND ANALYSIS

Generally, there are sufficient procedures, reviews and reconciliations to identify and manage potential risks to the TotalHR® system. However, some improvements can be made to system access rights, change management processes, and system security.

1. A few users have more system access than needed and authorizations can be improved.

TotalHR® 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. Access levels for at least five TotalHR® users exceed their day-to-day business needs.

Some employees' access to TotalHR® has not been based on the individual's regular job responsibilities and the principle of least privilege access. Least privilege access refers to providing only the system access necessary to perform one's job duties, which also limits potential risk exposure. At least five current users have more system access than necessary.

Currently four users have system administrator rights to TotalHR®. However, two of these users do not have regular responsibilities that would require system administrator access. Additionally, a generic system administrator user ID that is used for a particular function is shared among the four system administrators. As a result, individual responsibility could not be assigned in the event of an error. Because system administrator access provides powerful authority over the application, this level of access should be limited to the fewest number possible.

As well, three management-level employees have system access that allows them to update employee and benefit information. Each manager indicated they have supervisory responsibilities to review TotalHR® data and transactions, but do not have responsibilities or regular duties that include entering data or transactions.

B. TotalHR® functions have not been reviewed to ensure that incompatible duties are separated between two or more users.

Certain individuals currently have system access to update all employee and benefit information in TotalHR®. Additionally, data changes made by Payroll and HR staff are only reviewed by the same individual user who entered the data. Although the technology specialist reconciles pay rate changes each pay period, she relies on documentation provided by the same data entry staff.

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 TotalHR® functions as a whole.

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

Authorizations for system access and user access changes were not retained until recently. Although they are now retained, the authorizations are not easy to locate. Further, while TotalHR® displays the current access levels provided to current users, historical information is not available.

The system administrators grant TotalHR® access based on authorization from Payroll or Human Resources management. This authorization most often comes in the form of an email request. Until recently, the emails or other documentation supporting system access being provided, changed, or removed was not kept. However, now that the supporting authorization is retained, it is saved electronically in the pay period files when the change is effective rather than being centrally filed. As a result, locating system access authorization is difficult unless the authorization date is known. Keeping a log of system access authorizations or saving all authorizations in one folder would facilitate locating the documentation when needed.

As a result of system access changes not being tracked or logged 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. However, we reviewed the listing of all authorized TotalHR® users as of November 8, 2010, to ensure that there were not any former employees still authorized.

Quarterly, the technology specialist reviews authorized users for reasonableness. However, the Payroll and Human Resources managers who oversee the business functions of TotalHR® could more effectively review whether authorized users' system access remains appropriate given any changes in their job responsibilities.

Recommendations:

A. Payroll and HR management and the Financial Services Technology Director should review current users' TotalHR® system access for appropriateness based on the "least privilege" principle. Specifically, the Finance & Accounting technology staff should reduce the number of system administrators to the fewest possible. In addition, Payroll and HR management should authorize removal of unneeded data entry access rights.

B. Payroll and HR management should complete a segregation of duties analysis to ensure that one person cannot initiate, authorize, and complete a transaction from beginning to end in TotalHR®. This includes ensuring independent reviews of data changes.

C. The Finance & Accounting technology staff should ensure user access changes are logged and authorization documents can be located for each TotalHR® user. At least annually, Payroll and HR management should be provided a list of their authorized users with their access levels and certify that system access is commensurate with each user's current business needs.

2. Standardizing TotalHR® change management requirements would provide better assurance that changes have been properly authorized and tested.

The level of documentation maintained for TotalHR® application changes has been left to the discretion of the Finance & Accounting technology staff (system administrators) making the change. Consequently, business owner approval of TotalHR® business process changes and documentation of the testing of system changes is not always available. A technology change, such as a network-related update, would typically be initiated by IT staff. However, because an application like TotalHR® supports a key business function, the "business owner" (Payroll and HR) typically initiates and/or authorizes business-related changes, such as a new tax rate. The following areas can be improved:

- Currently, the TotalHR® system administrators record system changes in an Excel spreadsheet, listing the date of the change, the applicable pay period, a description of the change, and initials of the system administrator making the change. A system-generated log would provide better assurance of a complete record of changes made.
- Printed documentation of a change is usually maintained, and this sometimes includes the business owner approval. Requiring business owner approval would provide better assurance that the change is appropriately timed and necessary for business purposes.
- A test environment that mirrors the production environment is used by the system administrators for testing updates prior to introducing them in the production environment. However, documentation is not retained to show that a change was tested prior to it being implemented in the production environment, or the tests performed.

Because of the experienced system administrators, less formal procedures and documentation have been used to maintain TotalHR®.

Recommendation:

The Financial Services Technology Director, in conjunction with the City's IT Division, should establish a documentation standard for changes made to the TotalHR® application. At a minimum the standard process should require documentation of business owner approval of business-related changes, and testing of all changes prior to their move to the production environment.

3. Security improvements can be made to better protect TotalHR®.

Currently, TotalHR® password parameters do not require users to create a strong password for system access. In addition, improvements can be made in controls over user ID requirements, user login attempts, automatic timeouts, and concurrent sessions. Although TotalHR® has some system limitations, steps could be taken to improve current controls. These issues have been discussed more specifically with management and are not detailed in this public report.

Recommendation:

Management should fully utilize existing system parameters to assist in protecting the integrity, confidentiality, and availability of TotalHR®. Where system limitations exist, the TotalHR® vendor should be requested to consider system improvements.

ACTION PLAN

---

1. **A few users have more system access than needed and authorizations can be improved.**

   A. Access levels for at least five TotalHR® users exceed their day-to-day business needs.

   Recommendation: Payroll and HR management and the Financial Services Technology Director should review current users' TotalHR® system access for appropriateness based on the "least privilege" principle. Specifically, the Finance & Accounting technology staff should reduce the number of system administrators to the fewest possible. In addition, Payroll and HR management should authorize removal of unneeded data entry access rights.

   MANAGEMENT RESPONSE:
   Historically, the two management positions within Finance had system access levels set at a level equivalent or higher than their subordinates to enable them to cover job functions in the event staffing was unable to perform those functions. As dynamics have changed for the workflow and the platform, this approach should be reevaluated.

   As the TotalHR platform is shared by HR and Finance management has been working to enable both HR and Finance to have staff members that can affect changes to the platform as business needs change. Finance and HR management will need to reexamine the plan to enable the update access and the depth of support we were pursuing. Additional system training for HR staff will be needed to allow for cross Divisional support of the application.

   PROPOSED RESOLUTION:
   Finance and HR management will review the system access levels for the five users noted in the audit to determine if the reduction of their access levels will provide additional security benefits while not impeding their ability to perform their job functions.

   RESPONSIBLE PARTY:
   Finance and HR Management, Financial Services Technology Director

   COMPLETED BY: JANUARY 2011

   B. TotalHR® functions have not been reviewed to ensure that incompatible duties are separated between two or more users.

   Recommendation: Payroll and HR management should complete a segregation of duties analysis to ensure that one person cannot initiate, authorize, and complete a transaction from beginning to end in TotalHR®. This includes ensuring independent reviews of data changes.

   MANAGEMENT RESPONSE:
   TotalHR® functions are being reviewed to ensure that segregation of duties exists to ensure one person cannot initiate, authorize, and complete a transaction from beginning to end in TotalHR®. Controls in place include the review of Staffing Requisitions, Class

and Pay Plan Forms, Payroll Action Forms and Disciplinary Payroll Action Forms by Human Resources Staff and their subsequent signature authority to initiate the transaction. Finance does not initiate or authorize personnel transactions. Internal controls within the Payroll Department includes an independent review of all personnel transactions, balancing of hourly rates, and other edit reports by at least one other person than the person processing the transaction. Additional controls exist organizationally via the Position Control reports, validation through Document Management in Human Resources of the scanned documents initiating the transaction, and through other budgetary controls.

All system record changes are tracked via an audit log. The current audit log records all activity in the system versus just data entry, creating a cumbersome process to verify in its entirety. Staff currently reviews changes for only data entered.

PROPOSED RESOLUTION:
Finance and HR management will complete a formal segregation of duties analysis to determine if existing control processes could be improved.

Continue to work with the Technology staff on creating an audit log on only information keyed by staff. Develop a tighter control on the audit log process to ensure that all transactions are reviewed and approved by at least one independent person.

RESPONSIBLE PARTY:
Finance & HR Management (Payroll Manager, Human Resources Manager, Finance and Accounting Technology Staff)

COMPLETED BY: DECEMBER 2011

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

Recommendation: The Finance & Accounting technology staff should ensure user access changes are logged and authorization documents can be located for each TotalHR® user. At least annually, Payroll and HR management should be provided a list of their authorized users with their access levels and certify that system access is commensurate with each user's current business needs.

MANAGEMENT RESPONSE:
A process has already been initiated that retains documents relating each user's access and the authority who has requested the access change.

PROPOSED RESOLUTION:
The Finance & Accounting Technology staff will continue to expand a formal user access process for the platform. This expansion will include storing the information in an easier to access format for review. This formalized process will include a required annual review and approval of existing users by the appropriate management structure in additional to the quarterly review by Finance & Accounting technology staff.

RESPONSIBLE PARTY: Financial Services Technology Director

COMPLETED BY: FEBRUARY 2011

2. **Standardizing TotalHR® change management requirements would provide better assurance that changes have been properly authorized and tested.**

   Recommendation: The Financial Services Technology Director, in conjunction with the City's IT Division, should establish a documentation standard for changes made to the TotalHR® application. At a minimum the standard process should require documentation of business owner approval of business-related changes, and testing of all changes prior to their move to the production environment.

   MANAGEMENT RESPONSE:
   As noted in the audit, an existing system of tracking changes does exist, however the system is less formal than a traditional corporate or large government IT change management system. The existing system also relies on email or verbal direction to be given to staff when implementing business process changes. All changes are tested using our test platform by our most experienced staff in the area of the change. In order to provide a higher level of transparency to our processes, we see value in moving to a formal change management model.

   PROPOSED RESOLUTION:
   The Financial Services Technology director will work with the City's Information Technology Director to establish a formalized documentation process for business related changes made to the platform. The IT Division is implementing a new IT Service Management system that will enable a more universal, standardized change management policy across the organization. This platform will be used as the basis for the formalized change management process.

   RESPONSIBLE PARTY: Financial Services Technology Director, Information Technology Director

   COMPLETED BY: JANUARY 2012

3. **Security improvements can be made to better protect TotalHR®.**

   Recommendation: Management should fully utilize existing system parameters to assist in protecting the integrity, confidentiality, and availability of TotalHR®. Where system limitations exist, the TotalHR® vendor should be requested to consider system improvements.

   MANAGEMENT RESPONSE:
   Discussion with audit team highlighted several limitations of the platform security functions around user login attempts, concurrent sessions, inactivity timeouts, and user id requirements. While the security functions within TotalHR have some limitations they are compensated for by stronger security controls at the City Network and City Workstations security levels.

   The City maintains strong user logins, passwords, and inactivity timeout functions as part of the core City Network and City Workstation security infrastructure. These structures provide the first level of access control by preventing unauthorized users from accessing

the City Network.

Using this first layer of security, users are prevented from even launching the TotalHR unless they exist in the proper security access group. Once they launch TotalHR they are then prompted for a secondary login and password from the TotalHR system.

Most business applications within the City of Scottsdale directly rely on those functions using what's known as integrated security.

Integrated security means the business application relies on the network security for the primary security layer and does not use its own user-id / password system.

While the TotalHR platform is not capable of such integration at this time, its multi-layer security process is arguably more secure than most single layer integrated application security schemes. This in-turn functions as a compensating control for the limitations noted in the audit.

PROPOSED RESOLUTION:
The City will approach the vendor, AMSI, and determine if additional security functions can be integrated into the TotalHR platform to compensate for several of its security limitations. If the additional security functions can be added, the City will ask for a formal quote to make the modifications. From there a cost/risk analysis will be performed to determine the reasonableness of the modifications.

RESPONSIBLE PARTY: Financial Services Technology Director

COMPLETED BY: JUNE 2011

City Auditor's Office
4021 N. 75th St., Suite 105
Scottsdale, Arizona 85251
(480) 312-7756
http://www.ScottsdaleAZ.gov
Search: "auditor"

Audit Committee
Councilman Robert Littlefield, Chairman
Councilwoman Lisa Borowsky
Vice Mayor Suzanne Klapp

City Auditor's Office
Kyla Anderson, Senior Auditor
Joyce Gilbride, Assistant City Auditor
Lisa Gurtler, Assistant City Auditor
Erika Keel, Auditor
Joanna Munar, Senior Auditor
Lee Pettit, Senior Auditor
Sharron Walker, 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.