AUDIT REPORT

Audit of Management of User Access for the Human Resources Management System

September 2016

City of Austin

A Report to the Austin City Council

Office of the City Auditor

City Auditor
Corrie Stokes
CIA, CGAP, CFE

Deputy City Auditor
Jason Hadavi
CPA, CFE

REPORT SUMMARY

The Human Resources Department follows best practices and City policies for granting access and establishing password parameters for the Human Resources Management System. However, in order to fully ensure that the City's information is safeguarded against unauthorized access, current practices related to periodic review of user access, timely deletion of user accounts upon separation or transfer, and use of generic user accounts need to be further improved.

AUDIT NUMBER: AU15115
RELEASE DATE: SEPTEMBER 28, 2016

TABLE OF CONTENTS

Appendices

GOVERNMENT AUDITING STANDARDS COMPLIANCE

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.

AUDIT TEAM

Neha Sharma, CPA, CISA, CIA, Acting Assistant City Auditor
JoJo Cruz, CRMA, CICA, Auditor-in-Charge

Office of the City Auditor
phone: (512)974-2805
email: oca_auditor@austintexas.gov
website: http://www.austintexas.gov/auditor

Copies of our audit reports are available at http://www.austintexas.gov/page/archive-auditor-reports

Printed on recycled paper
Alternate formats available upon request

Audit Of Management Of User Access For The Human Resources Management System

September 2016

Report Highlights

Why We Did This Audit

This audit was conducted as part of the Office of the City Auditor's (OCA) FY 2015 Strategic Audit Plan.

This audit was selected based on the risk assessment of the City's systems.

What We Recommend

To strengthen the user access management process, the Director of HRD should establish processes for:

- Periodically reviewing of all system users and ensure that user access is based on business needs;
- Timely deletion of user accounts upon employee separation or transfer;
- Providing justification when generic accounts are created and establishing accountability for users of accounts.

For more information on this or any of our report e-mail
oca_auditor@austintexas.gov

BACKGROUND

The Banner Human Resources Management System is an enterprise-wide software application that supports the administrative functions related to human resources, payroll, and budget. City employees, whose job responsibilities require the use of this system, are granted access rights based on business needs.

The Human Resources Information System Division of the City's Human Resources Department is responsible for managing user access to this system. As of April 2016, there are approximately 700 user accounts with access rights to perform various department activities within the system.

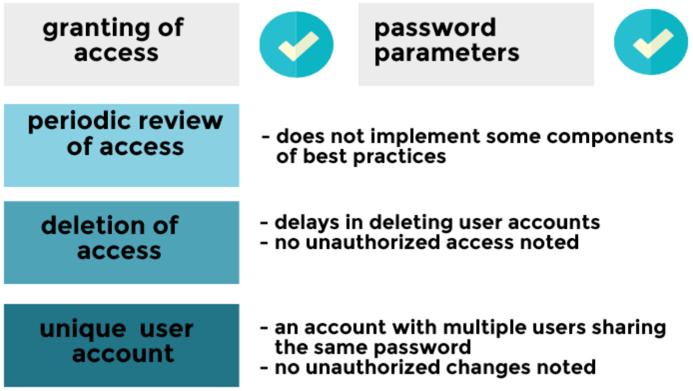
OBJECTIVE AND SCOPE

The objective of the audit was to determine whether access rights to the Human Resources Management System are properly managed to safeguard City's information and prevent unauthorized changes. The audit scope included review of City's current practices for user access management for the Banner Human Resources Management System.

WHAT WE FOUND

The Human Resources Department's processes for granting access to the Human Resources Management System and establishing password parameters follow best practices and City policies. However, in order to fully ensure City's information is safeguarded and prevented against unauthorized access or changes, current practices over the periodic review of users authorized to access the system, timely deletion of user accounts upon separation or transfer, and use of generic user accounts need to be further improved, as shown below.

Review of User Access Management for the Human Resources Management System



granting of access ✓

password parameters ✓

periodic review of access
- does not implement some components of best practices

deletion of access
- delays in deleting user accounts
- no unauthorized access noted

unique user account
- an account with multiple users sharing the same password
- no unauthorized changes noted

SOURCE: OCA analysis of user access management documentations, July 2016

BACKGROUND

The Banner Human Resources Management System is an enterprise-wide software application that supports the administrative functions of the City of Austin. This system has been in place since 1997, and has been used to facilitate day-to-day operations related to human resources, payroll, and budget.

City employees, whose job responsibilities require the use of this system, are granted access based on business needs. A user's role may change over the course of employment due to promotion, demotion, or transfer to another department. The Human Resources Information System Division in the Human Resources Department is responsible for managing users' access to the Human Resources Management System. As of April 2016, there are approximately 700 user accounts with access rights to perform various department activities within the system.

For this audit, we reviewed the user access management practices for this system. User access management includes procedures for the:

- granting of access to the system;
- establishment of secure password parameters for users;
- periodic review of user access to ensure that the access rights; are granted based on job responsibilities;
- deletion of user accounts upon separation or transfer; and
- assignment of unique accounts to each user.

OBJECTIVE, SCOPE, AND METHODOLOGY

The Audit of Management of User Access for the Human Resources Management System was conducted as part of the Office of the City Auditor's (OCA) Fiscal Year (FY) 2015 Strategic Audit Plan, as presented to the City Council Audit and Finance Committee. This audit was selected based on a risk assessment of various City's systems.

Objective

The objective of the audit was to determine whether access rights to the Human Resources Management System are properly managed to safeguard City's information and prevent unauthorized changes.

Scope

The audit scope included review of the City's current practices in place for user access management for the Banner Human Resources Management System.

Methodology

To accomplish our audit objectives, we performed the following steps:

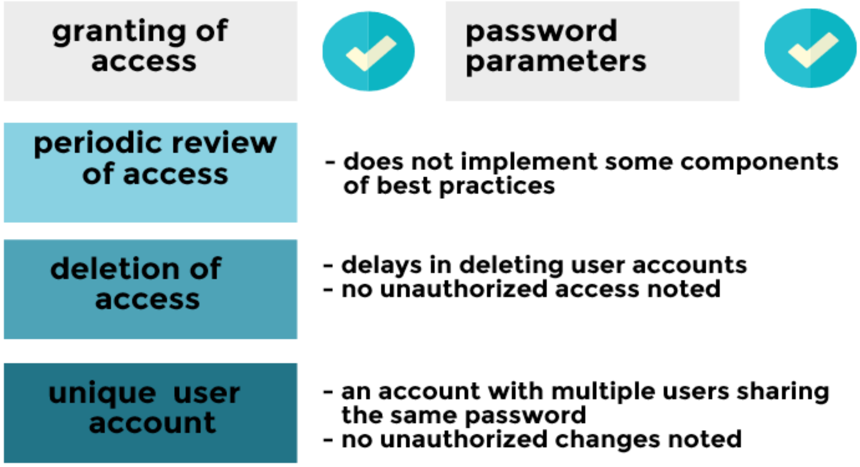
- reviewed Human Resources Department policies and procedures relating to user access management;
- conducted interviews with staff in the Human Resources Department and the Controller's Office;
- selected a judgmental sample of 10 Banner users for compliance with established policies and procedures, and verified if access rights are based on business needs;
- evaluated controls in place for periodic review of user access rights;
- verified whether access rights of 10 separated and 10 transferred Banner users were deleted on their last physical day of employment following separation or transfer;
- reviewed parameters used for securing user accounts;
- analyzed user accounts reports for identifying accounts shared by multiple users; and
- researched City policies and best practices for user access management. Specifically, we used the Institute of Internal Auditors' Global Technology Audit Guide for Identity and Access Management to evaluate user access management for the system.

WHAT WE FOUND

Finding: User access management for the Human Resources Management system is generally in compliance with best practices and City policies. However, improvements are needed in the current practices to ensure that City's information is safeguarded against unauthorized use.

The Human Resources Department follows best practices and City policies for granting access to the Human Resources Management System and establishment of password parameters. However, in order to fully ensure City's information is safeguarded against unauthorized access or changes, current practices regarding periodic review of user access, timely deletion of user accounts upon separation or transfer, and use of generic user accounts need to be further improved, as shown in Exhibit 1 below.

EXHIBIT 1
Review of User Access Management for the
Human Resources Management System



granting of access ✓

password parameters ✓

periodic review of access
- does not implement some components of best practices

deletion of access
- delays in deleting user accounts
- no unauthorized access noted

unique user account
- an account with multiple users sharing the same password
- no unauthorized changes noted

SOURCE: OCA analysis of user access management documentations, July 2016

Granting of access to the system generally complies with best practices.

granting of access

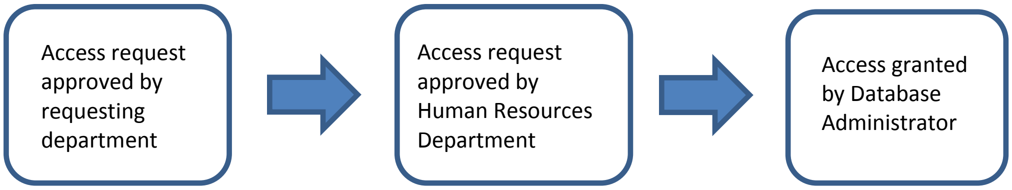
Best practices require that a user access request should be subject to multistep approval process

Best practices require that:

- initial access requests should be approved by the authorized individual directly responsible for supervising the requestor's activities;
- second level approval should be granted by the application owner; and
- after the appropriate approval has been secured, the system administrator should create the user account.

The Human Resources Department has established a process for granting users' access to the system based on recommended best practices as depicted in Exhibit 2 below. Our testing results indicated that this process is followed.

EXHIBIT 2
Access Approval Process



Access request approved by requesting department → Access request approved by Human Resources Department → Access granted by Database Administrator

SOURCE: OCA analysis of Human Resources Department request access and approval process, July 2016

Password parameters for the system generally complies with best practices and City policy.

Best practices and City's policy require that there should be a formal password policy to ensure security of passwords. Best practices require that:

- passwords should contain at least eight characters with a combination of alpha, numeric, and special characters;
- passwords must be changed periodically (e.g. after every 30 to 90 days) and automatically expire;
- not allow reuse of last 6 passwords; and
- the system should automatically lock after three to five failed attempts.

Human Resources Department has established these password parameters for system users.

password parameters

Best practices and City's policy require secure password attributes to access user accounts

While there is an established process to periodically review user access, the process lacks some elements of best practices, which increases the risk of unauthorized changes.

The Human Resources Department has established a process which require City departments to verify, on an annual basis, whether users need access to the system to perform their job responsibilities. We found that system users, other than those with programmer and help desk accounts, were consistently reviewed annually. However, we noted that there is no established requirement to review programmer accounts. There are 12 programmer and 17 help desk accounts for this system. For help desk accounts, Human Resources Department management asserted that the last review was performed two years ago. During the course of this audit, management reviewed and deleted 6 help desk and 1 programmer accounts because the accounts were no longer needed.

periodic review of access

Best practices require periodic review of user access for business needs

We also found that Human Resources Department does not have an established process to review additional access rights granted to system users. There are about 80 system users who have been granted additional access rights, such as rights to view and modify data. Of the 10 users we tested, 3 had access rights that were not required for performing their job responsibilities. Human Resources Department management deleted these excessive access rights during the course of this audit.

Further, Human Resources Department has no process to review the last log-in reports in order to identify inactive accounts, which could result from temporary/emergency accounts, and/or from separated or transferred employees' accounts that have not been deleted.

While there is a process for deleting system access for users, access has not been deleted timely upon separation or transfer, which increases the risk of unauthorized access to data.

deletion of access

City's policy requires that system access of separated or transferred employees be removed on their last physical day of separation or transfer

Sixteen out of the 20 separated and transferred users we selected for testing were not deleted on their last physical day prior to separation or transfer. Instead, Banner user accounts were deleted, on average, 11 days after the last day prior to separation or transfer. Human Resources Department staff asserted that City departments do not consistently communicate separation or transfer of users. As a result, Human Resources Department staff run weekly reports to extract separated and transferred employees in order to identify users whose accounts need to be deleted. Human Resources Department management stated that the separation or transfer of users are captured in the system based on the two-week payroll cycle; consequently, the weekly report does not capture all separations or transfers immediately.

In our review of a last log-in report, we did not find any unauthorized access by separated or transferred users in our sample.

A system account, with rights to modify data, and shared by multiple users with the same password (a generic account) limits the City's ability to identify and track user actions.

unique user account

City's policy requires each user be assigned a unique user ID

System users are generally assigned a unique account to ensure accountability of users' activities. However, we found a generic account shared by eight users, with the same password, which limits the City's ability to identify and track the actions of the users of this account. This account was created to provide timely and efficient processing of personnel update requests from various City departments, such as employees' classification changes or salary adjustments.

Human Resources Department management asserted that authorized users share this account in case a user working on a requested change becomes unavailable, enabling another user to take over the review and apply the needed change.

A waste report issued by our office in June 2016 noted that an employee received overtime pay despite not being eligible for overtime compensation. Because the generic account described above was used by a compensation consultant to apply the changes, accountability for the error could not be established. Since that time, Human Resources Department management reported closing access via the generic account and required the eight users of that account to use their own unique accounts to apply personnel updates from various City departments.

In addition, we noted that while the generic account was created to allow Human Resources Department employees to review requested changes from departments, the established access rights for the account also allowed for modification of information submitted by departments. We did not find any unauthorized changes to employees' job records using this generic account in our testing. During the course of this audit, the Human Resources Department adjusted the generic account access rights to no longer allow for modification of data and, as mentioned above, as of June 2016, management reported that this account is no longer in use.

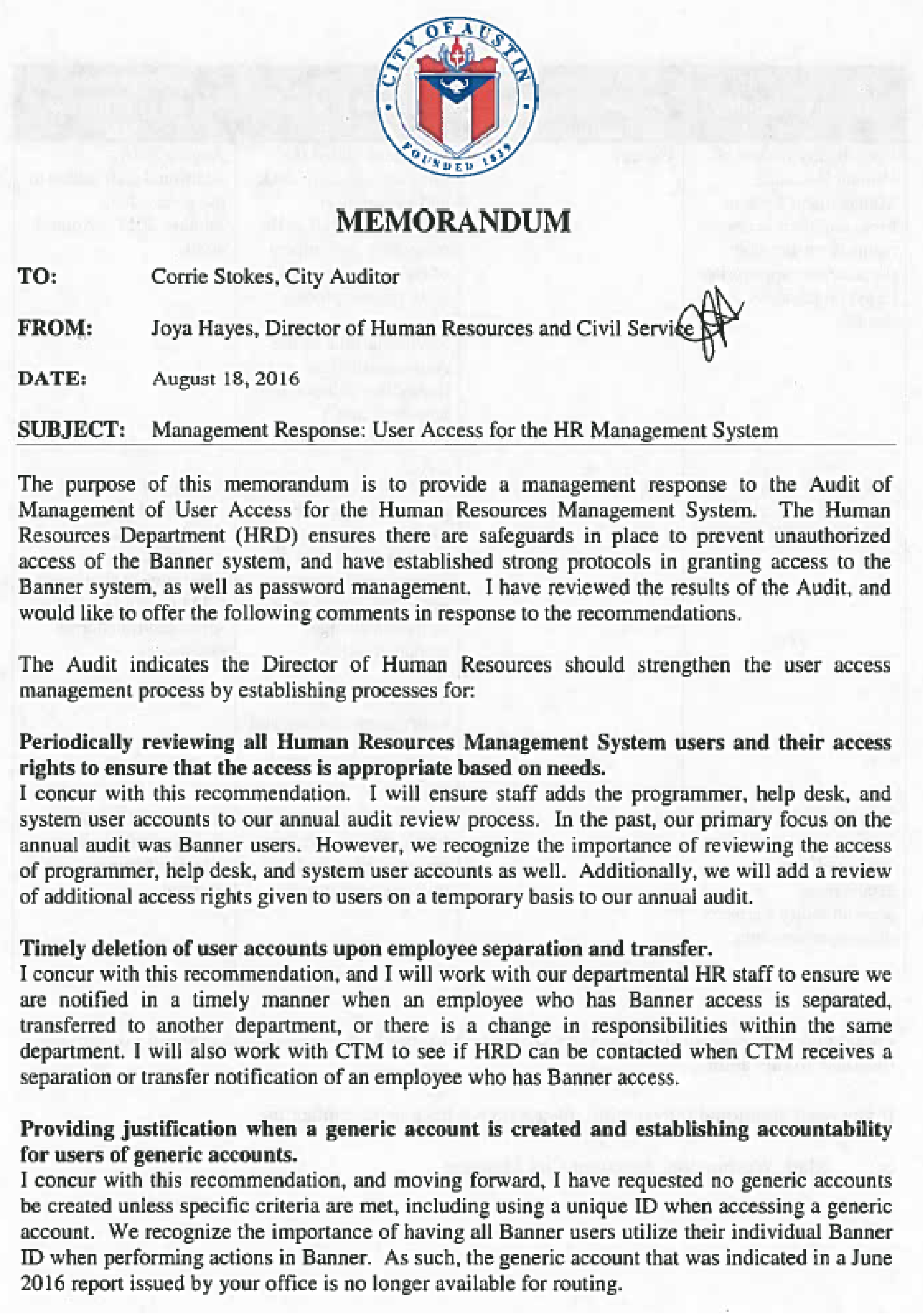
RECOMMENDATION

1. **The Director of Human Resources Department should strengthen the user access management process by establishing processes for:**
   - **periodically reviewing all Human Resources Management System users and their access rights to ensure that the access is appropriate based on business needs;**
   - **timely deletion of user accounts upon employee separation or transfer; and**
   - **providing justification when a generic account is created and establishing accountability for users of generic accounts.**

MANAGEMENT RESPONSE: Refer to Appendix A for management response and action plan.

APPENDIX A

MANAGEMENT RESPONSE



MEMORANDUM

TO: Corrie Stokes, City Auditor

FROM: Joya Hayes, Director of Human Resources and Civil Service

DATE: August 18, 2016

SUBJECT: Management Response: User Access for the HR Management System

The purpose of this memorandum is to provide a management response to the Audit of Management of User Access for the Human Resources Management System. The Human Resources Department (HRD) ensures there are safeguards in place to prevent unauthorized access of the Banner system, and have established strong protocols in granting access to the Banner system, as well as password management. I have reviewed the results of the Audit, and would like to offer the following comments in response to the recommendations.

The Audit indicates the Director of Human Resources should strengthen the user access management process by establishing processes for:

Periodically reviewing all Human Resources Management System users and their access rights to ensure that the access is appropriate based on needs.
I concur with this recommendation. I will ensure staff adds the programmer, help desk, and system user accounts to our annual audit review process. In the past, our primary focus on the annual audit was Banner users. However, we recognize the importance of reviewing the access of programmer, help desk, and system user accounts as well. Additionally, we will add a review of additional access rights given to users on a temporary basis to our annual audit.

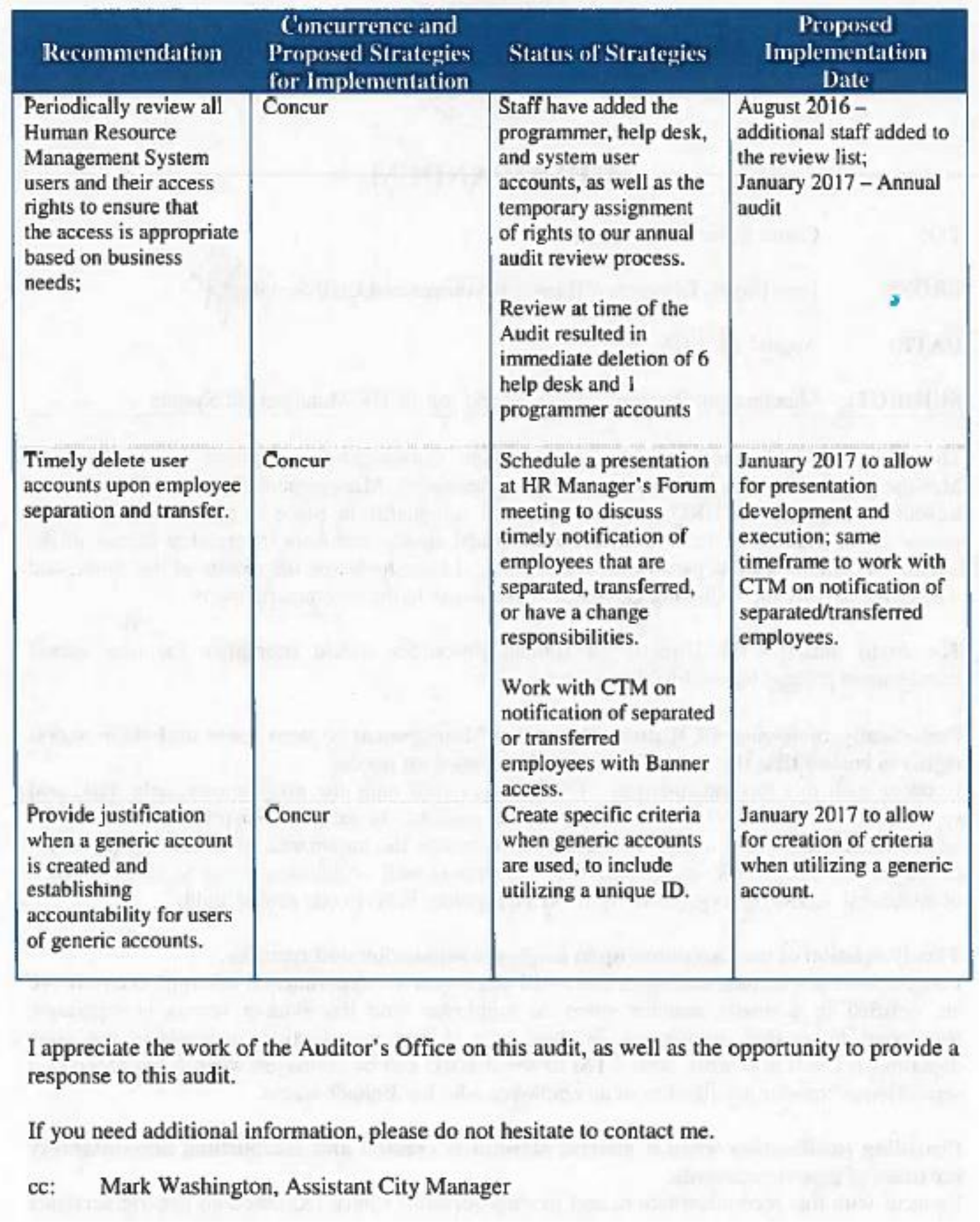
Timely deletion of user accounts upon employee separation and transfer.
I concur with this recommendation, and I will work with our departmental HR staff to ensure we are notified in a timely manner when an employee who has Banner access is separated, transferred to another department, or there is a change in responsibilities within the same department. I will also work with CTM to see if HRD can be contacted when CTM receives a separation or transfer notification of an employee who has Banner access.

Providing justification when a generic account is created and establishing accountability for users of generic accounts.
I concur with this recommendation, and moving forward, I have requested no generic accounts be created unless specific criteria are met, including using a unique ID when accessing a generic account. We recognize the importance of having all Banner users utilize their individual Banner ID when performing actions in Banner. As such, the generic account that was indicated in a June 2016 report issued by your office is no longer available for routing.

APPENDIX A

ACTION PLAN

Audit of Management of User Access for the Human Resources Management System



Recommendation	Concurrence and Proposed Strategies for Implementation	Status of Strategies	Proposed Implementation Date
Periodically review all Human Resource Management System users and their access rights to ensure that the access is appropriate based on business needs;	Concur	Staff have added the programmer, help desk, and system user accounts, as well as the temporary assignment of rights to our annual audit review process. Review at time of the Audit resulted in immediate deletion of 6 help desk and 1 programmer accounts	August 2016 – additional staff added to the review list; January 2017 – Annual audit
Timely delete user accounts upon employee separation and transfer.	Concur	Schedule a presentation at HR Manager's Forum meeting to discuss timely notification of employees that are separated, transferred, or have a change responsibilities. Work with CTM on notification of separated or transferred employees with Banner access.	January 2017 to allow for presentation development and execution; same timeframe to work with CTM on notification of separated/transferred employees.
Provide justification when a generic account is created and establishing accountability for users of generic accounts.	Concur	Create specific criteria when generic accounts are used, to include utilizing a unique ID.	January 2017 to allow for creation of criteria when utilizing a generic account.

I appreciate the work of the Auditor's Office on this audit, as well as the opportunity to provide a response to this audit.

If you need additional information, please do not hesitate to contact me.

cc: Mark Washington, Assistant City Manager