AUDIT REPORT

Workday User Access Controls

Multi-Agency

April 2019

Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O’Brien, CPA
Denver Auditor
Audit Team
Jared Miller, CISA, CFE, IT Audit Supervisor
Nicholas Jimroglou, CISA, Lead IT Auditor
Brian Cheli, CISA, CISSP, Senior IT Auditor
Joe Ebiziem, CISA, Senior IT Auditor

Audit Management
Timothy M. O’Brien, CPA, Auditor
Valerie Walling, CPA, CMC, Deputy Auditor
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Director

Audit Committee
Timothy M. O’Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000 ♦ Fax (720) 913-5253

Or download and view an electronic copy by visiting our website at: www.denverauditor.org.
AUDITOR'S LETTER

The objective of our audit of user access controls for Workday, the City and County of Denver’s accounting and human resources software application, was to evaluate the design and operational effectiveness of controls over all City user access to Workday—including how each agency adds, removes, and reviews user access. We found the Technology Services agency, the Office of Human Resources, and the Department of Finance need to establish a comprehensive governance structure, and the agencies also need to enhance user access security by addressing the considerations for additional controls that Workday advises for its customers and that are outlined in the 2018 Workday service organization controls report.

Through stronger governance and enhanced access controls, Technology Services, the Office of Human Resources, and the Department of Finance will be able to ensure the Workday application and its accompanying data are more secure. Our report lists several related recommendations to strengthen these processes.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, “General Powers and Duties of Auditor,” and was conducted in accordance with generally accepted government auditing standards. Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We extend our appreciation to the personnel from Technology Services, the Office of Human Resources, and the Department of Finance who assisted and cooperated with us during the audit. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor’s Office

Timothy M. O’Brien, CPA
Auditor
Objective
The objective of the audit was to evaluate the design and operational effectiveness of user access controls for Workday, the City’s accounting and human resources software application.

Background
Workday is a cloud-based software application for accounting and human resources management.

The City and County of Denver started using Workday in 2017 as its enterprise resource planning system for accounting functions and to manage human resources and payroll functions. Because Workday is cloud-based, the City’s more than 13,000 employees can access the application from any computer or mobile device through an internet connection.

Highlights
This is our first information technology audit focusing on user access controls for the City and County of Denver’s Workday software application since the City started using Workday in 2017.

We determined the City did not establish effective oversight of Workday after the application was implemented, which resulted in several customer requirements that have not been addressed.

The City Has Not Established Comprehensive Oversight of Workday to Ensure Effective Controls for User Access
We found that, because the City has not established comprehensive governance over Workday since its implementation two years ago and because the City has not established necessary internal controls to protect user access:

• The City lacks documented policies and procedures for Workday user access;
• Agencies are inconsistent in how they add new users and privileged users in Workday;
• The City performs no periodic reviews of user access other than for the proxy users of its test environments; and
• The City has not fully established a consistent review process related to conflicting job roles and the appropriate segregation of duties in Workday business processes.

For a copy of this report, visit www.denverauditor.org or contact the Auditor’s Office at (720) 913-5000.
# TABLE OF CONTENTS

## BACKGROUND

1

## FINDING

6

The City Has Not Established Comprehensive Oversight of Workday to Ensure Effective Controls for User Access

## RECOMMENDATIONS

14

## AGENCY RESPONSES TO AUDIT RECOMMENDATIONS

16

## OBJECTIVE, SCOPE, AND METHODOLOGY

19
BACKGROUND

Workday

Workday is a cloud-based software application for accounting and human resources management.\(^1\) It allows organizations to manage and integrate important day-to-day operations and is a critical component to agencies’ internal operations.

The City and County of Denver started using Workday in 2017 as its enterprise resource planning system for financial functions and to manage and update employee benefits, personal information, and payroll. Workday replaced the City’s previous enterprise resource system, PeopleSoft. The Office of Human Resources and the Department of Finance use the specific functions within Workday to perform various tasks. Additionally, the City’s Technology Services agency is responsible for supporting Workday.

Workday helps the City’s agencies—namely, the Office of Human Resources—recruit, manage, train, staff, and develop the City’s workforce of more than 13,000 employees from their hiring through their retirement. Workday also assists the City’s Department of Finance in managing the City’s payroll, financial, purchasing, accounting, and reporting of information necessary to operate and measure government operations, including budgeting and expenses.

Because it is a cloud-based application, the City’s Workday system can be accessed from any computer or mobile device with an internet connection, as illustrated in Figure 1. City employees log in to Workday using their secured user ID and password.

\(^1\) Cloud-based applications are traditionally commercial products. The City’s Workday software application is owned by Workday Inc.
Supervisors request Workday permissions to users after the user, as a prospective employee, completes the hiring and onboarding process. During the hiring process, a job applicant’s access in Workday is limited only to the job application process and any pre-employment information; they cannot access the City’s internal network until they complete the onboarding step in the hiring process.

The City’s general hiring process—depicted in Figure 2—starts in Workday’s recruiting module, where all job openings in the City are posted and viewable by the public. Job applicants create their own usernames and passwords to log in to the recruiting module and start the application process.

The City agency responsible for posting a given job opening reviews the applications submitted online and selects candidates for interviews with a hiring team. After interviews conclude, the agency prepares an offer of employment for its chosen candidate. Once the hiring agency approves the offer, the Office of Human Resources’ records team verifies whether the agency’s approval of that offer, as well as the hire date and start date, are appropriate.

After this review, Human Resources sends an email to the new hire with a hyperlink to Workday, where the individual must formally “accept” the job offer. After the new hire accepts the offer, Human Resources sends another link with the new hire’s employee ID number and a temporary password for the individual to complete their pre-employment paperwork in Workday.

Figure 3 above outlines the general process of how a job applicant-turned-new hire interacts with Workday.

While most City agencies follow this general hiring process, some use a different process.

For example, when hiring election judges, the Clerk and Recorder’s Office initiates a background check—conducted by a third party—before that prospective judge is given any access to Workday. If the prospective election judge passes their background check, only then does the Clerk and Recorder’s Elections Division ask the City’s Technology Services agency to complete the new hire’s onboarding in Workday.

Workday has two kinds of user-access permissions: role-based and user-based. Role-based permissions are tied to the position or job title an employee has, while user-based permissions are tied to the individual employee themselves.

**Role-Based Security** – After a new hire accepts a position in the City, they are assigned a “role” in Workday. A role is a security group assigned certain permissions, usually specific to an agency or organizational unit and tied to specific job functions. Employees assigned a specific role can see certain key data or perform certain actions in the Workday system based on that role. For example, the role

---

3 For the purposes of this report, the term “new hire” refers to either new City employees or new contingent or contracted workers.
for a Human Resources “recruiter” gives the employee in that position the permission to post job openings through the City’s recruiting portal in Workday or to review and revise that posting.

Role permissions are attached to each specific position, not the individual employee. Each role consists of a number of specific abilities in the system. For example, if a newly hired employee is assigned an “accounts payable” position with the ability to initiate payment for a customer invoice, that employee may also have the ability to initiate other processes in the scope of their job duties. But if that employee transferred to a different position or left their employment with the City, they would be removed from their assigned position and the permissions assigned would remain with that role. Once a new employee is hired to fill the vacancy, that new employee would then need to be assigned that same position to inherit the permissions their predecessor had.

**User-Based Security** – User-based security permissions are additional permissions that are not part of a Workday role and that are assigned to specific users. Security administrators in the City’s Technology Services agency grant user-based permissions, which typically involve elevated or sensitive permissions for a specific user only if that user needs this extra access. For example, if a City employee needs to view sensitive information for their job, they can be assigned specific user permissions by a security administrator that allow them to see the sensitive information.

The individual employee maintains their user-based security permissions even if they change positions, unless a security administrator explicitly changes the permissions, which is initiated through a task sent to the security administrator’s inbox. Changes to user-based permissions are logged through tickets in the City’s SupportNow system, which the City uses to document and resolve internal IT support requests.

**Proxy Users** – A subset of privileged users in Workday are “proxy users,” or users who have administrative access in the application’s test environments. Test environments are segregated from the production—or real-world—environment of a software application, but test environments still have copies of information and data (as of a certain point in time) from that live environment.

Proxy users are essential, because they test, edit, and review changes to Workday before those changes are officially implemented in the production environment.
Business Processes in Workday

Workday has “business processes,” which are a set of tasks users can initiate, act on, and complete to accomplish desired objectives. Users with appropriately assigned roles can initiate a business process, which then alerts other users of any tasks they need to do to complete the process.

For example, an accounting journal business process may require the user initiating the process to upload supporting documentation before Workday can move to the next step, or task, in the overall process.

All business processes are based on specific definitions, which are set by the City’s Workday administrators. Since Denver implemented Workday, the application has contained myriad business processes configurable to meet the City’s needs. The City can create versions of the same business process for different agencies or divisions and also specify custom definitions for each version, depending on each entity’s need.

Service Organization Controls Reports

A service organization controls, or SOC 1, report is intended to be a reference for an organization—such as the City and County of Denver—or entities auditing that organization’s financial records to use as assurance that internal controls at the organization are effective. Internal controls are policies, procedures, techniques, and mechanisms that help achieve an organization’s objectives and address identified risks.

The SOC 1 report provides a description of how the service organization—in this case, Workday—ensures its internal controls are achieved. One section of the report provides additional complementary policies, procedures, and controls that should be present and that are the responsibility of each customer—e.g. the City—to implement. For example, Workday’s 2018 SOC 1 report offers a section on “complementary customer controls,” which states in part that Workday customers are responsible for maintaining appropriate documentation to support all transactions processed by Workday.

FINDING

The City Has Not Established Comprehensive Oversight of Workday to Ensure Effective Controls for User Access

In 2018, an external audit firm provided Workday with a service organization controls, or SOC 1, report—verifying the effectiveness of Workday’s internal controls over processing its customers’ transactions, such as the City’s accounting and human resources transactions. The SOC 1 report also included a prescribed list of considerations—called “complementary customer controls”—that Workday customers, including the City and County of Denver, need to implement to ensure their data in Workday are correct.

However, our audit work revealed the City did not implement all the customer considerations from the SOC 1 report. This resulted in inconsistent procedures and user security concerns. Specifically, we found:

- Inconsistent processes for how agencies add new users and how they conduct reviews of user access;
- The City has not developed a consistent process to approve and remove privileged users from Workday to prevent sensitive information from being accessed for longer than is needed; and
- Limited evidence exists documenting that segregation-of-duties conflicts are reviewed before business processes change in Workday.

These problems exist ultimately because the City did not designate an individual or team to implement the recommended complementary controls detailed in Workday’s SOC 1 report. The City’s failure to implement these control considerations increases the risk the City’s data in Workday could be accessed by unapproved users.

The City Lacks Centralized Ownership for Workday

The City should implement the complementary controls detailed in the 2018 Workday SOC 1 report by formalizing policies, procedures, and additional control steps; however, we found no prescribed method for how that should be done.

We attribute this—and the resulting inconsistencies—to a lack of ownership by any City agency over the application itself. Specifically, the lack of centralized leadership or oversight has allowed the City’s agencies to each develop their own procedures without requiring
collaboration among them or consistency across their practices.

The National Institute of Standards and Technology recommends organizations establish a formal governance structure for information security to support the implementation of information security requirements. The institute says that information security governance should involve “establishing and maintaining a framework and management structure” that ensures information security efforts align with the organization’s objectives and are enforced through internal controls—such as policies and procedures—that the organization’s employees adhere to.

Subsequently, we found that because the City lacks this centralized governance for Workday, City agencies have inconsistent procedures regarding user access.

The City Lacks Consistent, Documented Processes for Adding and Formally Approving New Workday Users

The SOC 1 report advises that Workday customers, including the City, should control access rights for all users accessing the software application.

As discussed in the Background section, the City first grants users access to Workday during the hiring process. In our evaluation of the City’s processes for adding new users to Workday, we found there are no documented policies and procedures and, therefore, inconsistencies among City agencies in how users are granted access.

For example, we found:

- One prospective employee of the Clerk and Recorder’s Office retained an active Workday account—including network access—for 90 days after declining a job offer from the City;
- The Clerk and Recorder’s Office used a different process to grant user access and, as a result, five election judges had access to Workday before their background checks were validated; and
- Two City agencies—the Clerk and Recorder’s Office and the Denver Police Department—used email approvals resulting in five users being granted Workday access through only an email correspondence.

---

5 The National Institute of Standards and Technology is a laboratory and nonregulatory federal agency within the U.S. Department of Commerce.

Access Was Granted for Some Privileged Users without Documented Approval

Our audit work also identified a lack of evidence that formal approval was given before some administrative roles were set up.⁷

Formal approval requires a manager or supervisor to initiate a request ticket in ServiceNow, the City’s system for entering, tracking, and updating IT service requests. However, the requested level of a privileged user’s access and the period of time for this access is only sometimes required in the ServiceNow ticket.

Approval for new user requests is to be obtained and documented in the ticket. The manager or supervisor routes approved requests to a Workday security administrator in the City’s Technology Services agency, who creates the new account and closes the ticket. Figure 4 depicts this general process for setting up a privileged user’s account.

We requested evidence in the form of ServiceNow tickets to determine if there was appropriate approval prior to granting privileged access. Out of 45 privileged users selected, we noted a total of 494 roles associated with these users. Although Technology Services personnel told us that a process for approving privileged access exists, most roles we reviewed did not contain evidence to demonstrate that this approval does, in fact, exist.

Specifically, we found:

- There was no documented evidence provided for 264 roles supporting how the roles were assigned.
- There was no formal approval in ServiceNow requests before accounts for nine roles were set up.
- There was no formal documentation of approval for 57 roles before they were granted access; however, the risk associated with these users was mitigated, because the roles were

⁷ “Privileged users” are individuals who have been assigned elevated access. Administrators can have the highest level of elevated access, such as to maintain the system and promote changes to production, create and/or modify new or existing user account profiles, or create and/or modify financially significant employee or billing attributes.
revoked in a timely manner. Although some roles we reviewed were revoked and posed no risk at the time of our audit, City agencies still need proper documentation of these approvals for transparency and accountability.

The complementary customer control considerations in Workday’s SOC 1 report state that the City is responsible for controlling access rights as necessary for each user to accomplish their job responsibilities. Not implementing the complementary customer control considerations can result in City employees maintaining inappropriate access to Workday.

Some Proxy Users Were Not Properly Authorized for Privileged Access

Our audit work also found that “proxy users,” or users who have administrative access in the Workday test environments, were not properly authorized according to standard procedures explained to us by Technology Services personnel.

Proxy users are required to sign the City’s sensitive information policy before being granted access to the test environments. However, of the 10 proxy users we sampled for verification, there was no documentation for half to evidence they signed the policy.¹⁰

Although test environments are segregated from the live, production environment, proxy users have unrestricted ability to read data in these test environments—which can include copies of information or sensitive data from the production environment, such as personally identifiable information.¹¹ Users who are not properly authorized could potentially view sensitive information.

As stated, the complementary customer control considerations in the Workday SOC 1 report recommend controlling access rights necessary for each user to accomplish their job responsibilities. Therefore, the City should have consistent access controls for all proxy users.

The City Lacks a Formalized Process for Periodically Reviewing User Access

In addition to controlling access rights, the complementary customer control considerations also recommend Workday customers review security access and authorization limits on a periodic basis. However, we found the City lacks a formalized, consistent process to periodically

---

¹⁰ The City’s sensitive information policy authorizes certain employees, throughout the course of their job duties, to have the ability to “collect, generate, send, receive, view and/or otherwise use, have access to or become aware of personal or business information that is sensitive in nature, including personal, private or confidential data protected by law.”

¹¹ “Personally identifiable information” is any information about an individual maintained by a City agency, including any information that can be used to distinguish or trace an individual’s identity.
review access authorizations in Workday and assess whether they remain appropriate.

We found that the City’s Technology Services agency has taken steps to perform a review of one user group (proxy users). However, we found no evidence of any other City agency performing reviews of user access, as recommended by the Workday complementary customer control considerations.

We were informed that Technology Services plans to conduct a third-party security review of Workday, which will evaluate certain security features and controls in Workday beyond just user access.

If periodic reviews are not done, City employees—for example—could transfer between agencies and maintain user-based roles no longer relevant given their new position.

To address the City’s lack of oversight of the Workday software application and to address the resulting inconsistencies among agencies in how they address user access, we make the following recommendations.

**RECOMMENDATION 1.1**

**Establish the Governance Committee’s Authority** – The City’s Technology Services agency should collaborate with the Office of Human Resources and the Department of Finance to obtain the appropriate authority over Workday processes and procedures and to implement effective controls over user access as soon as possible for all agencies that use Workday. A committee could be established to incorporate input from each City agency to ensure consistent coverage citywide.

Agency Response: Agree, Implementation Date – June 30, 2019

**RECOMMENDATION 1.2**

**Implement Complementary Customer Control Considerations** – After implementing Recommendation 1.1, the City’s Technology Services agency should work with the established governance committee to develop and implement controls as soon as possible to address the complementary customer considerations outlined in the 2018 Workday service organization controls report.

Agency Response: Agree, Implementation Date – June 30, 2019
RECOMMENDATION 1.3

Perform Annual Review of Complementary Customer Control Considerations – After implementing Recommendation 1.2, the governance committee should incorporate an annual review of the complementary customer control considerations from future Workday service organization controls reports to ensure the City maintains effective internal controls for the application.

Agency Response: Agree, Implementation Date – June 30, 2019

RECOMMENDATION 1.4

Develop and Implement Policies and Procedures – After implementing Recommendation 1.1, the governance committee should develop and implement policies and procedures for user access as soon as possible. These policies and procedures should be based on standards in the National Institute of Standards and Technology’s Special Publication 800-53, fourth revision, to further prevent inconsistencies in how user access is maintained.

Agency Response: Agree, Implementation Date – June 30, 2019

City Agencies Do Not Consistently Review for Segregation-of-Duties Conflicts in Workday

We also reviewed how the City manages conflicts in Workday regarding the segregation of duties. Segregating duties in an organization prevents errors and fraud by ensuring at least two individuals are responsible for completing a task.

Specifically, we analyzed how City agencies identify, review, and prevent potential conflicts in user access. We found that, while some agencies—such as the Office of Human Resources—do analyze and document potential segregation-of-duties conflicts in Workday, not all agencies are reviewing for these potential conflicts.

The Office of Human Resources developed a matrix that aligns different positions in the office with various Workday business processes under the office’s purview. As discussed in the Background section, a “business process” is a set of tasks in Workday users can initiate, act on, and complete to accomplish desired objectives. Human Resources’ matrix document allows for a high-level review of potential conflicts that might arise when creating new business processes or assigning Workday roles.
to a business process. Such a potential conflict might be when one user can initiate a business process in Workday and also approve that same process.

Meanwhile, the Department of Finance incorporated a third-party review of the business processes in Workday before the business processes were implemented in the department’s Workday production environment. During the City’s initial implementation of Workday, consultants met with Finance personnel and personnel from other City agencies because of changes to business processes. Despite these meetings, though, none of the agencies were able to provide formal documentation for the third-party review regarding rationale for how business processes were implemented.

An actions matrix, or segregation-of-duties workbook, is a recommended practice for managing user access by both the American Institute of Certified Professional Accountants and the Information Systems Audit and Control Association, which are globally accepted, industry-leading associations that provide knowledge and best practices for controlling user access. The American Institute of Certified Public Accountants specifically expresses the need for not only developing a segregation-of-duties workbook for each “framework,” or best practices for an industry, but also for maintaining the workbook as changes occur to personnel and business processes.

Maintaining appropriate segregation of duties in Workday is a delicate balance between the rules in the business processes and the specific actions allowed by users’ roles. A change in one business process may create potential segregation-of-duties issues in a different business process. For example, the business process to create and approve a new vendor should not allow an individual user to approve a new vendor and also approve payment to that same vendor. Such a violation of segregation of duties could be caused by one individual having two different roles with incompatible duties. Because these interrelationships are complex, they need to be documented and maintained in a workbook whenever changes are made to a business process or job role. All changes to business processes should also be reviewed and tested to ensure segregation-of-duties conflicts are not created by these changes.

Because of City agencies’ inconsistency in reviewing for segregation-of-duties conflicts in Workday, we make the following recommendation to

---


ensure potential conflicts do not arise as a result of changes to business processes in the application.

RECOMMENDATION 1.5

Develop and Implement Procedures for Segregation-of-Duties Considerations – After implementing Recommendation 1.4, the governance committee should incorporate guidance as soon as possible so that agencies’ considerations of segregation of duties are documented and tested by the agency responsible whenever there is a change to a Workday business process.

Agency Response: Agree, Implementation Date – August 31, 2019
RECOMMENDATIONS

1.1 Establish the Governance Committee’s Authority – The City’s Technology Services agency should collaborate with the Office of Human Resources and the Department of Finance to obtain the appropriate authority over Workday processes and procedures and to implement effective controls over user access as soon as possible for all agencies that use Workday. A committee could be established to incorporate input from each City agency to ensure consistent coverage citywide.

Agency Response: Agree, Implementation Date – June 30, 2019

Agency Narrative: Technology Services established a governance committee prior to selecting Workday as the City’s ERP with representatives from each functional area, including Human Resource, Finance and Payroll, Procurement, Technology Services, and the Airport. The committee meets regularly to address system issues and enhancements, security and other aspects of the Workday System. Technology Services will work with the governance committee to develop and implement more thorough Workday processes and procedures and to implement effective internal controls over user access used by all agencies.

1.2 Implement Complementary Customer Control Considerations – After implementing Recommendation 1.1, the City’s Technology Services agency should work with the established governance committee to develop and implement controls as soon as possible to address the complementary customer considerations outlined in the 2018 Workday service organization controls report.

Agency Response: Agree, Implementation Date – June 30, 2019

Agency Narrative: The Workday Governance Committee believes the vast majority of the complementary customer controls are in place. The Committee will develop, implement and document the remaining controls.

1.3 Perform Annual Review of Complementary Customer Control Considerations – After implementing Recommendation 1.2, the governance committee should incorporate an annual review of the complementary customer control considerations from future Workday service organization controls reports to ensure the City maintains effective internal controls for the application.

Agency Response: Agree, Implementation Date – June 30, 2019

Agency Narrative: The Workday Governance Committee will monitor the complementary customer controls on an annual basis, with the first review taking place as indicated in recommendation 1.2.
1.4 **Develop and Implement Policies and Procedures** – After implementing Recommendation 1.1, the governance committee should develop and implement policies and procedures for user access as soon as possible. These policies and procedures should be based on standards in the National Institute of Standards and Technology’s Special Publication 800-53, fourth revision, to further prevent inconsistencies in how user access is maintained.

**Agency Response: Agree, Implementation Date – June 30, 2019**

Agency Narrative: The Workday Governance Committee will finalize the policies and procedures for user access based on NIST SP 800-53r4.

1.5 **Develop and Implement Procedures for Segregation-of-Duties Considerations** – After implementing Recommendation 1.4, the governance committee should incorporate guidance as soon as possible so that agencies’ considerations of segregation of duties are documented and tested by the agency responsible whenever there is a change to a Workday business process.

**Agency Response: Agree, Implementation Date – August 31, 2019**

Agency Narrative: The Workday Governance Committee will provide guidance to the business owners to ensure that segregation of duties is considered and documented within the change control process.
AGENCY RESPONSES TO AUDIT RECOMMENDATIONS

April 9, 2019

Auditor Timothy M. O’Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O’Brien,

The Office of the Auditor has conducted a performance audit of Workday User Access Controls.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was initially sent to us on March 14, 2019. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
The City Has Not Established Comprehensive Oversight of Workday to Ensure Effective Controls for User Access

RECOMMENDATION 1.1
Establish the Governance Committee’s Authority – The City’s Technology Services agency should collaborate with the Office of Human Resources and the Department of Finance to obtain the appropriate authority over Workday processes and procedures and to implement effective controls over user access used by all agencies, as soon as possible. A committee could be established to incorporate input from each City agency to ensure consistent coverage citywide.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>June 30, 2019</td>
<td>Chad Mitchell</td>
</tr>
<tr>
<td></td>
<td></td>
<td>720-913-4953</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.1
Technology Services established a governance committee prior to selecting Workday as the City’s ERP with representatives from each functional area, including Human Resource, Finance and Payroll, Procurement, Technology Services, and the Airport. The committee meets regularly to address system issues and enhancements, security and other aspects of the Workday System. Technology Services will work with the governance committee to develop and implement more thorough Workday processes and procedures and to implement effective internal controls over user access used by all agencies.
### Implement Complementary Customer Control Considerations

After implementing Recommendation 1.1, the City’s Technology Services agency should work with the established governance committee to develop and implement controls, as soon as possible, to address the complementary customer considerations outlined in the 2018 Workday service organization controls report.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>June 30, 2019</td>
<td>Chad Mitchell 720-913-4953</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.2**

The Workday Governance Committee believes the vast majority of the complementary customer controls are in place. The Committee will develop, implement and document the remaining controls.

### RECOMMENDATION 1.3

**Perform Annual Review of Complementary Customer Control Considerations** – After implementing Recommendation 1.2, the governance committee should incorporate an annual review of the complementary customer control considerations from future Workday service organization controls reports to ensure the City maintains effective internal controls for the application.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>June 30, 2019</td>
<td>Chad Mitchell 720-913-4953</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.3**

The Workday Governance Committee will monitor the complementary customer controls on an annual basis, with the first review taking place as indicated in recommendation 1.2.

### RECOMMENDATION 1.4

**Develop and Implement Policies and Procedures** – After implementing Recommendation 1.1, the governance committee should develop and implement policies and procedures for user access, as soon as possible. These policies and procedures should be based on standards in the National Institute of Standards and Technology’s Special Publication 800-53, fourth revision, to further prevent inconsistencies in how user access is maintained.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>June 30, 2019</td>
<td>Chad Mitchell 720-913-4953</td>
</tr>
</tbody>
</table>
Narrative for Recommendation 1.4

The Workday Governance Committee will finalize the policies and procedures for user access based on NIST SP 800-53r4.

RECOMMENDATION 1.5
Develop and Implement Procedures for Segregation-of-Duties Considerations – After implementing Recommendation 1.4, the governance committee should incorporate guidance, as soon as possible, so that agencies’ considerations of segregation of duties are documented and tested by the agency responsible whenever there is a change to a Workday business process.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>August 31, 2019</td>
<td>Chad Mitchell 720-913-4953</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.5
The Workday Governance Committee will provide guidance to the business owners to ensure that segregation of duties is considered and documented within the change control process.

Sincerely,

David Eddinger
Chief Information Officer

cc: Christine Binnicker, Deputy Chief Information Officer
    Brendan Hanlon, Chief Financial Officer
    Karen Niparko, Executive Director of Human Resources
    Beth Machann, City Controller
    Kelli Bennett, Director of Accounting and Financial Reporting
    Chris Longshore, Director of Human Resources Technology and Innovation
    Chad Mitchell, Executive Director of Applications
    Jacquelyn Pyun, Workday Program Administrator
    Tricia Scherer, IT Governance Manager

    Valerie Walling, Deputy Auditor, CPA, CMC®
    Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Manager
    Jared Miller, CISA, CFE, IT Audit Supervisor
OBJECTIVE

The objective of the audit was to evaluate the design and operational effectiveness of user access controls for Workday, the City’s accounting and human resources software application.

SCOPE

The scope of the audit was limited to user access for Workday application systems—particularly for new users added from August 2018 to January 2019, for privileged users in place from January 2016 to January 2019, and for proxy users in place from January 2018 to January 2019.

Specifically, the audit sought to review Workday’s 2018 service organization controls report and whether the City:

- Authorizes and appropriately establishes access for new Workday users;
- Appropriately removes Workday access from terminated users;
- Appropriately authorizes and manages administrative access in Workday;
- Properly reviews access for current Workday users;
- Has clearly defined the segregation of business process roles in Workday;
- Restricts proxy user access to only authorized individuals; and
- Appropriately configures password settings for Workday users.

METHODOLOGY

We applied various methodologies to gather and analyze information related to our audit objective.

These included:

- Reviewing our office’s 2017 Workday conversion payroll audit to gain an understanding about the issues related to our audit objective;\(^{12}\)
- Reviewing complementary customer controls from the 2018 Workday service organization controls report;
- Reviewing policies and procedures related to logical access controls in Workday;
- Interviewing key personnel in the City’s Technology Services agency, Office of Human Resources, Department of Finance, Civil Services Commission, Clerk and Recorder’s Office, and Department of Public Safety, as well as the Denver Public Library;

• Determining if new and administrative users are appropriately approved to access Workday prior to them being given access; and
• Determining if Workday password settings are appropriately configured.
Office of the Auditor

The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies and contractors for the purpose of ensuring the proper and efficient use of City resources. He also provides other audit services and information to City Council, the Mayor, and the public to improve all aspects of Denver’s government.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City’s finances and operations, including the reliability of the City’s financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000 ♦ Fax (720) 913-5253
www.denverauditor.org

Our Mission

We deliver independent, transparent, and professional oversight in order to safeguard and improve the public’s investment in the City of Denver. Our work is performed on behalf of everyone who cares about the City, including its residents, workers, and decision-makers.