Audit Team

Jared Miller, CISA, CFE, Audit Supervisor
Nicholas Jimroglou, CISA, Lead IT Auditor
Joe Ebiziem, CISA, Senior IT Auditor

Audit Management

Timothy M. O’Brien, CPA, Auditor
Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, 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.

Cover photo by Denver Auditor’s Office staff.
June 4, 2020

AUDITOR’S LETTER

In keeping with generally accepted government auditing standards and Auditor’s Office policy, as authorized by city ordinance, the Audit Services Division has a responsibility to monitor and follow up on audit recommendations to ensure city agencies address audit findings through appropriate corrective action and to aid us in planning future audits.

In our follow-up effort for the “Workday User Access Controls” audit report issued in April 2019, we determined the Technology Services agency, the Office of Human Resources, and the Department of Finance fully implemented most of the recommendations we made in the original audit report. Despite the agencies’ efforts, auditors determined the risks associated with the audit team's initial findings have not been fully mitigated. As a result, the Audit Services Division may revisit these risk areas in future audits to ensure the city takes appropriate corrective action.

The Highlights page in this report provides background and summary information about the original audit and the completed follow-up effort. Following the Highlights page is a detailed implementation status update for each recommendation.

I would like to express our sincere appreciation to the personnel in the Technology Services agency, the Office of Human Resources, and the Department of Finance who assisted us throughout the audit and the follow-up process. 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 from Original Audit
This was 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 had not established effective oversight of Workday after the application was implemented, which resulted in several customer requirements that were not addressed.

The City Has Not Established Comprehensive Oversight of Workday to Ensure Effective Controls for User Access
We found that, because the city had not established comprehensive governance over Workday since its implementation [in 2017] and because the city had not established necessary internal controls to protect user access:

- The city lacked documented policies and procedures for Workday user access;
- Agencies were inconsistent in how they added new users and privileged users in Workday;
- The city performed no periodic reviews of user access other than for the proxy users of its test environments; and
- The city had not fully established a consistent review process related to conflicting job roles and the appropriate segregation of duties in Workday business processes.

REPORT HIGHLIGHTS

<table>
<thead>
<tr>
<th>FULLY IMPLEMENTED</th>
<th>PARTIALLY IMPLEMENTED</th>
<th>NOT IMPLEMENTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
While the Technology Services agency, the Office of Human Resources, and the Department of Finance implemented three recommendations made in the “Workday User Access Controls” audit report, one recommendation was only partially implemented and another has yet to be acted upon.

By fully implementing three of our recommendations, the Technology Services agency is now ensuring oversight of the city's use of the Workday application, and it is ensuring effective internal controls are in place for user access. This remediation by Technology Services helps address the security risks associated with the city's data in Workday and helps prevent unauthorized users from accessing that information.

However, the risk remains that Technology Services will not address all changes or new complementary customer control considerations in future service organization controls reports because a review of these controls is not performed.
**FINDING | 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 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 ACTION**

Original target date for completion: June 30, 2019

In response to our recommendation, the city created the Workday Governance Committee, a committee charter, a change control charter, a Workday security policy, and a Workday security process document to further strengthen program governance after the Workday implementation and to document decisions made by the Workday Governance Committee.

The committee charter, created in June 2019, outlines the authority and responsibilities of the Workday Governance Committee, which is now the city’s authority over Workday policies and procedures. We inspected the charter and found personnel from several key agencies across the city collaborated to develop these responsibilities. These included: the Controller’s Office, the Technology Services agency, the Office of Human Resources, Denver International Airport, and supply chain management personnel.

The city also created a Workday stakeholder group to advise, discuss, and share ideas for improvements on Workday-related topics with governance committee members. This group includes 28 people from key leadership positions across the city.

Because city agencies collaborated to create a formal Workday Governance Committee and develop appropriate authority through a charter, a policy, and a procedure, we consider this recommendation fully implemented.
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 ACTION**

*Original target date for completion: June 30, 2019*

After the city established the Workday Governance Committee in accordance with Recommendation 1.1, the Technology Services agency worked with the committee to develop policies and procedures to address the complementary customer considerations outlined in the Workday service organization controls report.

We found each complementary customer consideration corresponds to a relevant policy or procedure to address each risk area. For example, one of the responsibilities for Workday customers, outlined in the complementary customer considerations, recommends that user access be reviewed periodically. We determined the city’s Workday security policy includes details about the frequency of security reviews, who is responsible for performing the reviews, and the various user groups that will be reviewed. This was further evidenced by inspecting the 2019 fourth quarter proxy review, which demonstrated a review was performed and required changes or deletions to proxy user accounts were applied.

Therefore, we consider this recommendation fully implemented.

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 ACTION**

*Original target date for completion: June 30, 2019*

As mentioned in the agency action for Recommendation 1.2, the Technology Services agency collaborated with the Workday Governance Committee to
develop internal controls to address the complementary customer control considerations outlined in the Workday service organization controls report. However, when we asked Technology Services personnel about the extent of an annual review of these complementary customer control considerations, we were informed no such review is performed.

Technology Services personnel told us this recommendation should not have been agreed to in the original audit. This was Technology Services' response to the recommendation when the original report was issued in April 2019:

*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.*

Even though Technology Services personnel told us they are not reviewing the complementary customer control considerations on an annual basis as they had agreed to last year, they provided evidence that Technology Services performs annual risk reviews of the Workday service organization controls report. However, these annual risk reviews did not provide explanations or evidence of what the review was meant to document or what the reviewer was doing during the process.

Reviews for service organization controls are important. However, Technology Services' efforts did not address the risk that changes or new complementary customer control considerations in future service organization controls reports might be missed and, thus, not implemented.

Therefore, we consider this recommendation not implemented.

**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 ACTION**

**Original target date for completion: June 30, 2019**

As mentioned in the agency action for Recommendation 1.1, the Technology Services agency collaborated with the Office of Human Resources and the Department of Finance to obtain the appropriate authority for the Workday Governance Committee and its charter. We reviewed the charter and
determined the Workday Governance Committee now has the overarching authority to develop and implement policies, practices, and internal controls over the city's Workday system.

Since June 30, 2019, the Workday Governance Committee developed and implemented a Workday security policy and a security process for the city's Workday user access. The policy and process includes guidelines for provisioning and de-provisioning user access and for periodically reviewing user access in the city's Workday system. These guidelines help mitigate the risks around unauthorized user access controls by defining how access permissions are managed, the frequency of reviews, and the teams responsible for removing access when an employee leaves their job with the city.

Additionally, the Workday security policy specifies that for Workday user access, the Workday Governance Committee must adhere to the National Institute of Standards and Technology's Special Publication 800-53, fourth revision. Auditors corroborated guidelines in the city's Workday security policy with those in the Special Publication 800-53 — which recommends that organizations should review user accounts for compliance with account management and define a frequency for that review.

Therefore, we consider this recommendation fully implemented.

**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 ACTION**

**Original target date for completion: Aug. 31, 2019**

In response to our recommendation, the Workday Governance Committee created a Workday security policy and a charter for its Workday Change Control Board to address segregation-of-duties considerations. However, when we reviewed these documents, we found the Workday security policy and the charter of the Workday Change Control Board contained limited detail related to segregation-of-duties considerations.

For example, the charter includes a brief sentence to verify there are no segregation-of-duties violations, but it does not provide any other details such as how conflicts will be evaluated, considerations of least
privileged access, and other factors the National Institute of Standards and Technology's Special Publication 800-53, fourth revision, recommends.

Because of the limited language and lack of details, we asked personnel from the Technology Services agency about how Technology Services is considering segregation-of-duties conflicts for business process changes. Before answering our questions, Technology Services personnel requested additional time so they could prepare an updated Workday Change Control Board Charter, which they provided us on May 6, 2020. After reviewing the updated charter, we found Technology Services added additional details related to how segregation-of-duties violations will be considered, and it now aligns with the Special Publication 800-53.

The updated charter demonstrates Technology Services’ progress. However, for auditors to consider this an authorized document, the charter still needs to be signed by Technology Services management.

Additionally, we were told the Workday Governance Committee evaluates segregation-of-duties conflicts based on the committee members’ professional judgment when there is a business process change. If they determine a conflict exists, the Workday Governance Committee members decide how best to proceed with the business process change. Technology Services personnel told us that when a business process change is approved, this indicates Technology Services evaluated the change in accordance with the language in the Workday Change Control Board Charter. The Workday Governance Committee does not implement the business process change if it determines there are any segregation-of-duties conflicts during the review.

After evaluating the evidence provided and after interviewing Technology Services personnel, we determined the Workday Governance Committee is considering segregation-of-duties conflicts when a Workday business process change occurs. However, because the updated Workday Change Control Board Charter has not been officially authorized, we consider this recommendation only partially implemented.
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.

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.