TECHNOLOGY & INNOVATION
ORACLE POST IMPLEMENTATION REVIEW
AUDIT 23-11
AUGUST 25, 2023

City of Tampa
Jane Castor, Mayor

Internal Audit Department
315 E. Kennedy Boulevard
Tampa, Florida 33602
Office (813) 274-7159

August 25, 2023

Honorable Jane Castor
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: Oracle Post Implementation Review, Audit 23-11

Dear Mayor Castor:

Attached is the Internal Audit Department's report on Oracle Post Implementation Review.

The Department of Technology & Innovation (T&I) has already taken positive actions in response to our recommendation. We thank the management and staff of T&I for their cooperation and assistance during this audit.

Sincerely,

/s/ Christine Glover

Christine Glover
Internal Audit Director

cc: John Bennett, Chief of Staff
Dennis Rogero, Chief Financial Officer
Russell Haupert, Director of Technology & Innovation
Donald Disler, MIS Project Leader
David Clement, Lead Systems Analyst
Kenneth Marshall, Lead Systems Analyst
Carl Brody, Assistant City Attorney

TECHNOLOGY & INNOVATION
ORACLE POST IMPLEMENTATION REVIEW
AUDIT 23-11
AUGUST 25, 2023

/s/ Stephen Mhere
_____
Senior Auditor

/s/ Vivian Walker
_____
Lead Senior Auditor

/s/ Christine Glover
_____
Audit Director

TECHNOLOGY & INNOVATION
ORACLE POST IMPLEMENTATION REVIEW
AUDIT 23-11

BACKGROUND

The City of Tampa (COT)'s Enterprise Resource Planning Modernization Project (migration from Oracle E-Business Suite to Oracle Cloud services) was completed in November 2021. Oracle Cloud enables COT to perform computing activities with the help of Oracle Corporation under Infrastructure as a Service (IaaS) and Software as a Service (SaaS) agreement. The Technology & Innovation Department (T&I) has a full-time staff of seven, working under a project leader, dedicated to Oracle Cloud.

STATEMENT OF OBJECTIVE

This audit was conducted in accordance with the Internal Audit Department's FY 2023 Audit Agenda. Its objective was to determine if the system of internal controls relating to the use of Oracle Cloud was adequate.

STATEMENT OF SCOPE

The audit period covered activities that occurred after Oracle Cloud was implemented in November 2021. We reviewed these activities to determine if T&I and other COT departments that use Oracle Cloud were fulfilling their duties and responsibilities in an effective and efficient manner. Original records were used as evidence and verified through observation and physical examination.

STATEMENT OF METHODOLOGY

We accomplished our audit objective as follows:

- Evaluated internal controls related to Oracle Cloud, including a review of relevant policies.
- Reviewed the contract between COT and the vendor that provides cloud computing services.
- Interviewed the Management Information Systems Project Leader to discuss his perspective of fraud and disparity risk within the Oracle Implementation Team.
- Surveyed department users of applications that interface with Oracle Cloud to determine their perception of system performance since Oracle Cloud was brought into operation.
- Assessed data processed in Oracle Cloud for reliability.

- Reviewed Tampa.gov, Intranet, and budget books for Oracle Cloud performance metrics. There are currently no relevant post implementation performance metrics for Oracle Cloud.

STATEMENT OF AUDITING STANDARDS

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.

NOTEWORTHY ACCOMPLISHMENTS

T&I successfully replaced all core business systems from an outdated infrastructure and technology base to the cloud hosted system expeditiously. This involved moving financial, procurement, Human Resources, and payroll systems within 10 months. According to cloud computing industry experts, the average time to complete large-scale cloud migration projects such as this is about 16 months.

AUDIT CONCLUSION

Based upon the test work performed and the audit finding noted below, we conclude that the system of internal controls relating to the use of Oracle Cloud is adequate. However, information captured in some of the system's audit logs is inconsistent and needs to be improved.

AUDIT LOGS

STATEMENT OF CONDITION: There are more than 4,700 user accounts set up in COT's cloud computing platform. Most of these users are COT employees, but others are associates of the cloud service provider. When needed, sometimes user accounts for external auditors are created to provide them with limited access to the application.

The cloud computing application has been set up to generate audit logs. Audit logs are a historical record of activities in a system – they contain information such as who did what and when. In our review of audit logs, we found that most of them do provide information relating to who created or updated user passwords in the system. However, there were inconsistencies in the audit logs: identities of users who created or updated some passwords are anonymous.

CRITERIA: Best practice standards for internal controls for information security recommend that system or audit logs should include sufficient information to determine the events that occurred as well as who, and/or what, caused them.

CAUSE: We consulted with T&I but could not readily determine the cause. T&I is researching the issue.

EFFECT OF CONDITION: The purpose of audit logs is to provide data for computer forensics or cybersecurity analysis. If audit log data are insufficient for that purpose, identifying malicious users or threat actors becomes much more difficult, thereby reducing the effectiveness of audit logs as a detective security control.

RECOMMENDATION: We recommend T&I work with the cloud computing vendor to implement a more effective audit log functionality by making sure that all logs identify users who create/update user passwords and any other data in the system.

MANAGEMENT RESPONSE: The audit log in question is a report on password changes in Oracle. Modifying a password can be done in one of three sanctioned ways. In some cases, the audit log for a forgotten password reset will display "anonymous" rather than the actual username. In working with Oracle, we have determined that the system is working as designed and in such a case we have validated the change is from the link sent to the user for password reset.

While we can recommend and advocate for changes with the software developer, this functionality is not under the direct control or free for modification by the City. We will register an additional service request with Oracle and provide feedback to the Oracle development team.

Additionally, we will be moving Oracle access to Okta single sign-on in the very near future. This will take advantage of user network accounts and add Multifactor for general access. Any external password resets in the future will require MFA and provide full logging.

TARGET IMPLEMENTATION DATE: We entered the enhancement request with Oracle to capture the username on forgotten password resets on 8/4/2023. The Okta implementation with single sign-on to Oracle with MFA is currently scheduled for go-live on 12/1/2023.