Crowe

Smart decisions. Lasting value.™

City of Cupertino, California
Interim Audit Results

July 17, 2018

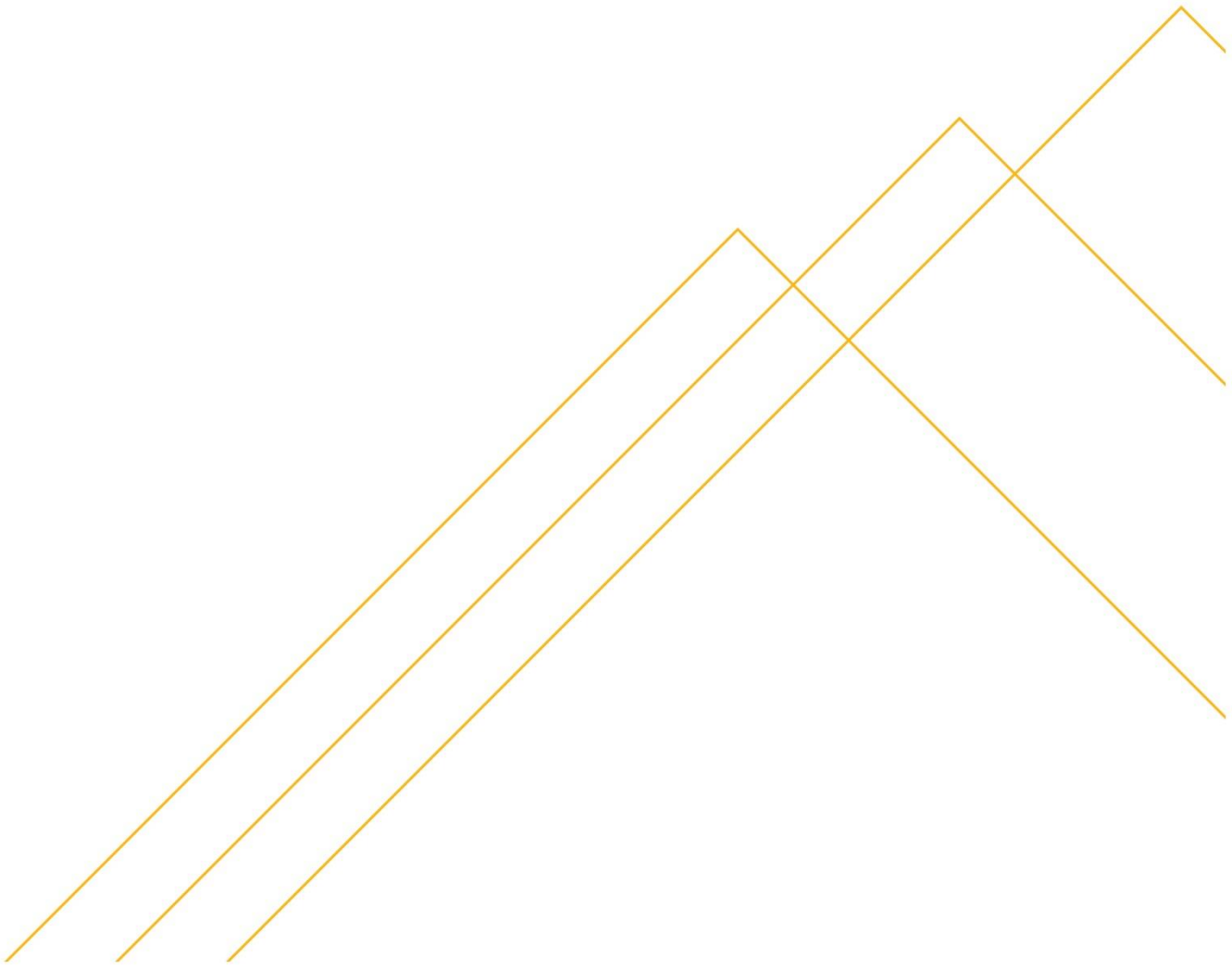

Table of Contents

Interim Audit Results

2018-001 – Information System Controls

Criteria: Internal controls over information systems are a key component of an organization's control environment. Entities should have internal controls including policies and procedures regarding user access, change management, and back-up and recovery. Where adequate segregation of duties cannot be employed via system access restrictions, detective and monitoring review controls should be established that adequately mitigate such risks. Such controls enable entities to increase efficiency by reducing manual processes and improving the accuracy and quality of the data used across those information systems. Such controls are also important to prevent erroneous and fraudulent transactions or entry to systems.

Condition: We evaluated system access to the City's Active Directory as well as the financial reporting system, New World Systems (NWS). The Active Directory authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is an authorized user.

During our assessment of the City's information system controls, we noted the following:

Financial Reporting System/Active Directory

- There is one user in the Finance Department who maintains super user access. Super user access includes the ability to add/modify/delete user accounts as well as assign security privileges to user accounts.
- The City's information and technology (IT) and finance departments do not have a process to evaluate the propriety of changes to user access within the financial reporting system. For example the City's IT department did not remove access to information systems in a timely manner for terminated employees. It is the City's intent that user access is removed immediately at separation date. We tested the timeliness of removal for 11 employees with termination dates after 1/1/2018. Of those 11 employees:
    - 3 user accounts were deactivated between 2 and 4 days after termination date
    - 2 user accounts were deactivated between 83 and 88 days after termination.
    - 1 user account was deactivated 102 days after termination.

Policies and Procedures

- The City's information technology policies and procedures have not been recently updated to reflect the practices that are currently in use. The City recently began to review the IT policies and procedures but have not made document changes. For example, areas such as the disaster recovery plan and internet access and use monitoring policy, are no longer applicable to the City due to changes in hardware, software and/or management structure, yet are still presented therein.

Cause:

Financial Reporting System/Active Directory

- Super user access was granted to the individual, as management had not yet identified a position within the City, but outside the finance department, which could permanently fulfill this role.
- User access requests for the financial reporting system are informal, typically verbal or through email. The City does not have a mechanism for tracking when user access is changed. Within the financial reporting system, the City has not yet identified the key reports which should be utilized to evaluate changes made to user access As such, the use of this informal process led to the delays in the user access change processing, as the City IT department was not timely notified of the requested changes.

Policies and Procedures

- With regard to the City's IT policies and procedures, there have been systematic changes to the City's disaster recovery plan, and other IT areas which have not yet been carried forward into the City's written policies.

Effect:

Financial Reporting System/Active Directory

Improper user access could result in fraudulent and/or unauthorized transactions being recorded in the City's financial reporting system, where management would not be able to detect such activity.

Policies and Procedures

Outdated policies and procedures may not provide the City a mechanism to restore critical information systems should there be a disaster recovery event. Further, in the event that key IT employees separate from the City, outdated policies and procedures may deter the City's ability to smoothly transition responsibilities to successors.

Recommendation:

Financial Reporting System/Active Directory

- The City should establish written policies and procedures which provide for the appropriate levels of user access based on the relative roles and responsibilities within the financial reporting system. A best practice is to provide the lowest level of access based on operational need. Further, we recommend the City perform a systematic review and maintain documentation of user's access rights within the financial reporting system, to ensure that a) there are not users with super user access who also have the ability to perform operational functions within the financial reporting system and b) users access roles are only for those functions which are necessary to perform in the normal course of business. Finally, we recommend that the City continue its efforts to implement a formal user access change to ensure that timely user access changes are processed.

Policies and Procedures

- We recommend that the City update its policies and procedures to reflect current conditions and establish a process to ensure periodic review occurs. IT policies should be reviewed and approved by management or those charged with governance on a periodic basis.

Management's Response and Planned Corrective Action:

Management agrees with auditor's recommendation. The City's Business Systems Analyst was transferred from the Innovation and Technology department to the Administrative Services department in April 2018. The position maintained administration rights (the ability to initiate system user-access changes); however, the City ensured the following:

- The Business Systems Analyst was never granted access or ability to enter transactions in the New World ERP system (NWS).

- NWS-generated control log reports were created on May 21, 2018, indicating (1) the Business Systems Analyst position had not transacted in the system during FY 2017-18, (2) the “NWS” user profile had not transacted in the system in FY 2017-18, and (3) all user-access changes made by the Business Systems Analyst were clearly identified and time-stamped.
- The Business Systems Analyst did/does not have physical access or custody to City assets.

As of June 29, 2018, administration rights/access has been removed from the Business Systems Analyst in Finance.

Although written policies and procedures have been drafted, it does not appear that a City-wide cognizance or adherence to said policies and procedures has been achieved. Currently, Finance staff is collaborating with members of the Innovation and Technology (I&T) Department to update and revise the policies and procedures to ensure controls are implemented, operating effectively, and monitored appropriately.

Upon the anticipated termination of an employee, the City’s Human Resources Division is currently requesting from I&T that all user access be removed and any other City property or City access belonging to the employee be returned prior to termination date.

Status of Prior Year Audit Findings

2017-001 – Information System Controls

Finding Summary:
During our evaluation of system access to the City's Active Directory as well as the financial reporting system, New World Systems (NWS), super user access was noted as well. In addition, revocation of access rights for a sample of terminated employees was not documented. Finally, policies and procedures had not been updated to reflect current practices in use.

Status of Corrective Action:
This finding has been repeated and included as finding 2018-001.

2017-002 – Timely Processing of Bank Reconciliations

Finding Summary:
Due to previously reported material unreconciled variances, the City deployed significant resources to correct the reconciliations through the end of the fiscal year ended June 30, 2017. As a result of that effort, bank reconciliations were not completed timely (i.e. 30 days subsequent to the end of the applicable reporting period).

Status of Corrective Action:
During our interim procedures, we noted that the bank reconciliations selected via a random sample during the interim period were completed timely with no material unreconciled differences. As a result, this finding was not repeated.

2017-003 – Prior Period Restatements for Pensions and Capital Assets

Finding Summary:
As a result of the audit procedures for the fiscal year ended June 30, 2017, prior period restatements were required to be reported due to errors identified in reporting of capital assets and pension-related items.

Status of Corrective Action:
These items will be reviewed during the audit of the financial statements for the fiscal year ended June 30, 2018.