



# CITY OF PALO ALTO OFFICE OF THE CITY AUDITOR

June 24, 2019

The Honorable City Council  
Palo Alto, California

## Policy and Services Recommends the City Council Accept the ERP Planning: Separation of Duties Audit

The Office of the City Auditor recommends acceptance of the ERP Planning: Separation of Duties Audit. At its meeting on October 23, 2018, the Policy and Services Committee approved and unanimously recommended that the City Council accept the report. Additionally, the Policy and Services Committee recommended a broader discussion with the City Council of this audit, ERP Planning: Data Standardization Audit, and the ERP Planning: Information Technology Data Governance Audit. In response to that request, on April 1, 2019, the Information Technology Department provided a review of the ERP system status in an informational report to City Council ([Staff Report ID # 9826](#)).

[The City Auditor's report to the Policy and Services Committee](#) and the [transcript minutes](#) are available on the City's [Policy and Services Committee website](#).

Respectfully submitted,

Don Rhoads, CPA  
Special Advisor to the Office of the City Auditor  
Management Partners

### ATTACHMENTS:

- Attachment A: Separation of Duties Audit (PDF)

Department Head: Don Rhoads, Special Advisor to the Office of the City Auditor





CITY OF  
**PALO  
ALTO**

# ERP Planning: Separation of Duties

October 17, 2018



## Office of the City Auditor

**Harriet Richardson**, City Auditor

**Mimi Nguyen**, Senior Performance Auditor

**Lisa Wehara**, Performance Auditor II

**Jordan Christenson**, Performance Auditor

Page intentionally left blank for double-sided printing



# OFFICE OF THE CITY AUDITOR

## EXECUTIVE SUMMARY

### ERP Planning: Separation of Duties

#### October 17, 2018

#### PURPOSE OF THE AUDIT

The purpose of this audit was to evaluate the adequacy of separation of duties for various activities in the current SAP system and make recommendations to ensure that any identified deficiencies are corrected for the new ERP system.

#### REPORT HIGHLIGHTS

<p><b>Finding:</b></p> <p><b>Implementing effective separation of duties and ensuring well-restricted user access controls for the new ERP system will decrease vulnerabilities and risks</b></p>	<p>The City uses varying automated and manual processes for separating key business activities and duties among staff for the high-risk activities we reviewed, such as payroll processing, purchase orders and check processing, revenue collections, and asset management transactions. Although we did not find any major concerns, we identified opportunities for improvement. We assessed an employee's ability to access and perform transactions within high-risk areas. We also offered an understanding of where the high-risk areas are within various workflows.</p> <p><b>Key Recommendation:</b></p> <p>When implementing the new ERP system, the Administrative Services, Information Technology, and Utilities Departments should separate duties for high-risk conflicting tasks by restricting transaction codes or developing mitigating controls where conflicts cannot be avoided.</p>
---	---

Page intentionally left blank for double-sided printing

## TABLE OF CONTENTS

Objective.....	1
Background.....	1
Scope .....	3
Methodology .....	3
Finding:	
Implementing effective separation of duties and ensuring well-restricted user access controls for the new ERP system will decrease vulnerabilities and risks. ....	5
Recommendations .....	14
Appendix 1: City Manager’s Response .....	15

### ABBREVIATIONS

ACFE	Association of Certified Fraud Examiners
AP	Accounts Payable
ASD	Administrative Services Department
ERP	Enterprise Resource Planning
FISCAM	Federal Information System Controls Audit Manual
IT	Information Technology
RC	Revenue Collections
RFP	Request for Proposal
SoD	Separation of Duties

Page intentionally left blank for double-sided printing



## INTRODUCTION

---

### Objective

The purpose of this audit was to evaluate the adequacy of separation of duties for various activities in the current SAP system and make recommendations to ensure that any identified deficiencies are corrected for the new Enterprise Resource Planning (ERP) system.

### Background

An ERP system is a type of business management software that integrates key business activities of the City, such as purchasing, inventory, utilities, accounting, payroll, and information technology. SAP is the current ERP system and has been in place since 2003. The city issued a Request for Proposal (RFP) and plans to complete migrating the City's business data and processes into a new ERP system by June 2022.

### Separation of Duties (SoD)

Separation of duties (SoD), also known as segregation of duties, is an internal control mechanism to reduce the risk of erroneous or fraudulent transactions, improper program changes, and the damage or destruction of computer resources. This is accomplished by separating parts of a process or activity across a department or organization. To reduce the risk of unauthorized transactions (intentional or unintentional), work responsibilities and the corresponding computer access should be segregated so that one individual does not control multiple critical stages of a process. For example, a person should not be allowed to enter an invoice for payment, approve an invoice for payment, process the invoice for payment, and disburse a check for payment. Doing so would result in an opportunity for that individual to create and process an unauthorized payment transaction.

### Standards and Guidance

We used the ISACA report, "Best Practices to resolve Segregation of Duties conflicts in any ERP environment," to document high-risk conflicting tasks in ERP systems and how they can be mitigated with automated separation of duties within the system, and developed criteria, which is explained below in the methodology section.<sup>1</sup>

For general guidance on separation of duties, we referred to the "Standards for Internal Control in the Federal Government," sections 10.12 - 10.14: Segregation of Duties, published in September 2014 by the United States Government Accountability Office. These sections give

---

<sup>1</sup> ISACA previously stood for Information Systems Audit and Control Association, but now goes by its acronym only. It is an independent, nonprofit, global association that engages in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems.

general guidance on the role of segregation of duties for internal control and the option for alternative control activities if separation of duties is not practical due to staffing limitations or other factors.

We referenced and used as guidance the “Federal Information System Controls Audit Manual” (FISCAM), sections 3.2: Access Controls and 3.4: Segregation of Duties, published in February 2009 by the United States Government Accountability Office, to generally assess the City’s control systems. It states that “effective segregation of duties starts with effective entitywide policies and procedures that are implemented at the system and application levels.”

### *Risk of not Implementing SoD*

According to a 2016 report on occupational fraud and abuse by the Association of Certified Fraud Examiners (ACFE), asset misappropriation was the most common form of occupational fraud.<sup>2</sup> Among the various forms of asset misappropriation, billing schemes and check tampering schemes were reported as posing the greatest risk.

In an ERP system, risks and vulnerabilities may arise from the lack of proper segregation of duties. Unintended risks often stem from granting employees excessive system authorizations by providing access to functions that are not within their official duties. Challenges can occur with the lack of resources, both financial and staffing.

Therefore, planning for the division of responsibilities and reflecting it in the access privileges granted through an automated process to users of Information Technology (IT) systems, as well as implementing manual processes to mitigate any residual risk, such as collusion, becomes necessary for the proper, efficient, and secure execution of the business processes.

### *SoD Responsibility*

The responsibility of SoD in the City resides within each business process area and within the IT systems supporting their execution. An effective SoD strategy requires that each business area, with a thorough understanding of its business process and workflow, collaborate with IT to gain an understanding of the system supporting SoD so the business area can structure and help IT design ERP security around separation of duties issues, particularly in the highest-risk areas.

---

<sup>2</sup> Under the Occupational Fraud and Abuse Classification System (Fraud Tree), asset misappropriation includes the theft of cash receipts and fraudulent disbursements, such as billing schemes, expense reimbursement schemes, check tampering, and register disbursements. Statistics included in the ACFE’s report are based only on the results of the single largest fraud case that certified fraud examiners self-reported in an online survey sponsored by the ACFE.

---

## Scope

We reviewed best practices for separation of duties for ERP systems and used criteria to assess the highest areas of risk to the City. Because this audit is intended to provide high-level guidance, we did not review and assess SoD for all workflow processes. We only identified the highest-risk areas and made recommendations for use as the City implements the future ERP system.

---

## Methodology

To accomplish our objective, we:

- Researched and identified SoD best practices and guidance.
- Created separation of duties criteria matrices from the list of high-risk conflicting tasks in ISACA's document, "Best Practices to resolve Segregation of Duties conflicts in any ERP environment," for six areas:
  1. Accounts Payable
  2. Payroll/Human Resource
  3. Revenue Collections
  4. Treasury
  5. Utilities
  6. Information Technology
- Identified active employees, their user profiles, and their executable transactions in SAP.
- Reviewed and analyzed conflicting tasks within the high-risk list.
- Discussed with staff any mitigating processes that address active users who have conflicting tasks.
- Determined the effectiveness of the mitigating processes, both automated and manual.

## How to Use This Report

Criteria matrices are presented for each business area we analyzed, which we developed based on ISACA's "Best Practices to resolve Segregation of Duties conflicts in any ERP environment." Each matrix displays the employee roles and responsibilities, separated by key tasks within the business area, and identifies the optimum separation of duties to mitigate high-risk conflicts.

The criteria matrices should be used as guidance to understand the conflicting tasks within a business area and where automation would be beneficial in the new ERP system to prevent employees from performing high-risk conflicting tasks. Exhibit 1 shows an example of a criteria matrix and how to read it. The intent of this report is to identify areas of highest risk, identify mitigating controls currently in place, and encourage the use of system automation to mitigate such risks.

**EXHIBIT 1**  
**Example Criteria Matrix with Auditor Explanation of How to Read**

Task number for identifying tasks

Task the employee performs

Read matrix from top to bottom for each employee to identify conflicting tasks

Task No.	Task Description	Employee performing task		
		E1	E2	E3
<i>Revenue Collections</i>	<i>Operations</i>			
1	Cash application	X		
2	Bank reconciliation		X	
3	Maintain bank master data			X

High risk tasks identified in ISACA

Employee should not perform task.

Employee should not perform task (not addressed on ISACA list).

Other tasks that the employee should not perform

**Mitigating Examples:**  
 If E1 can perform Task 1 & 2, they are able to steal cash without it being noticed. A mitigating manual control would be to have a supervisory review and approval prior to bank deposit.

Although these practices are recommended, full implementation may not be possible due to constraints such as ERP configuration, City budget, staffing, or other resource factors, in which case, manual controls may need to be substituted in lieu of automated processes.

**Compliance with government auditing standards**

We conducted this audit of ERP Separation of Duties in accordance with our FY 2017 and FY 2018 Annual Audit Work Plan and 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.

We would like to thank management and staff in the Information Technology, Administrative Services, and Utilities Departments for their time, cooperation, and assistance during the audit process.

## Finding

**Implementing effective separation of duties and ensuring well-restricted user access controls for the new ERP system will decrease vulnerabilities and risks.**

---

### Summary

The City uses varying automated and manual processes to separate key business activities and duties among staff for the high-risk activities we reviewed, such as payroll processing, purchase orders and check processing, revenue collections, and asset management transactions. Although we did not find any major concerns, we identified opportunities for improvement. We assessed an employee's ability to access and perform transactions within a high-risk area. We also offered an understanding of where the high-risk areas are within various workflows.

---

### ACCOUNTS PAYABLE

**Accounts Payable (AP)** is a division of the Administrative Services Department (ASD). Their goal is to process, record, and report citywide financial transactions. AP primarily uses SAP to maintain and process vendor invoices and payments. In FY 2017, the City issued 10,301 checks, and purchased \$122 million of goods and services. AP has four employees: a Senior Accountant, a Lead Account Specialist, and two Account Specialists.

Based on the matrix we developed in Exhibit 2, nine conflicting tasks would need to be performed by at least nine different employees for maximum separation of duties. Because this is not feasible with the four employees currently in AP, manual controls are needed to mitigate the high risks in this work area.

**EXHIBIT 2**  
**Accounts Payable**

Task No.	Task Description	Employee performing task								
		E1	E2	E3	E4	E5	E6	E7	E8	E9
<b>Accounts Payable</b>	<b>Operations</b>									
1	Maintain bank master	X								
2	Process vendor invoices		X							
3	AP payments			X			X			
4	Maintain asset master				X					
5	Maintain vendor master					X				
6	Create manual checks			X			X			
7	Maintain purchase order							X		
8	Bank reconciliation								X	
9	Purchase order approval									X

Employee should not perform task.  
Employee should not perform task (not addressed in ISACA).

**Mitigating Examples:**

If E7 can perform Task 2 & 7, they can purchase unauthorized items for personal use without being noticed. A mitigating manual control would be to require supervisory approval for approving vendor invoices.

**SOURCE:** Auditor's analysis and summary of ISACA's "Best Practices to resolve Segregation of Duties conflicts in any ERP environment."

*Accounts Payable employees can enter an invoice and process payment to that invoice, which creates an unnecessary risk*

While other departments enter invoices into SAP for AP staff to process, creating a separation of duties, occasionally AP staff processes their own invoices. All three Accounting Specialists in AP can enter an invoice and process the payment for supervisory approval. This creates a separation of duties conflict because payment may be made on a fraudulently created and entered invoice. User access allows invoices to be entered through three types of SAP transactions, each differing based upon the type of invoice entered for payment. Discontinuing AP's access to these SAP transactions and transferring this task to ASD Administration, for example, would immediately mitigate this high risk.

We reviewed other high-risk areas on the ISACA list for AP and determined that they are well separated and well administered.

**PAYROLL/HUMAN RESOURCES**

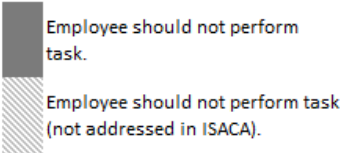
**Payroll** is a division of ASD that primarily processes payroll for city employees through timesheet and check processing. Paychecks are processed for about 1,200 employees, and total \$116 million dollars in authorized salary and benefits. Payroll has five employees: a Senior Accountant, an Accountant, two Payroll Analysts, and a Management Specialist.

Based on the matrix we developed in Exhibit 3, five conflicting tasks would need to be performed by at least four different

employees for maximum separation of duties. Staffing levels are sufficient with five employees in Payroll for effective separation of duties.

**EXHIBIT 3**  
**Payroll**

Task No.	Task Description	Employee performing task			
		E1	E2	E3	E4
<b>Payroll</b>	<b>Operations</b>				
1	Maintain master data	X			
2	Enter/change pay rates				
3	Process payroll		X		
4	Maintain time data			X	
5	Approve time				X



Mitigating Examples:

If E1 can perform Task 1 & 2, they can steal payroll money by increasing their own hourly rate without being noticed. A mitigating manual control would be to require supervisory review and approval of any changes made to pay rates.

**SOURCE:** Auditor's analysis and summary of ISACA's "Best Practices to resolve Segregation of Duties conflicts in any ERP environment."

**Payroll employees have access to all payroll operations, which creates risk**

Each City employee enters time into a timesheet system. A supervisor approves the time entered and Payroll approves and processes the timesheets for payroll processing.

Four of the five payroll employees have access to all payroll operations, for all employees and themselves. This is a high-risk access because it allows the ability to modify employee master data or salary information and then process payroll fraudulently.

Some high-risk tasks that should have restrictions, separation, or effective manual processes instituted, currently do not. These tasks allow for potential fraudulent activity, including the ability for Payroll staff to:

- Change their own and each other's salary data, which would allow the salary increase to go unnoticed.
- Change employee time data by entering fraudulent time to increase regular or overtime pay.
- Enter false personnel data and time to process a fraudulent payroll.

Although Payroll has a manual process in place to manage the risk of employees modifying master data and fraudulently processing the change through payroll, the control can be more effective. There may be opportunities within the new ERP system to automate or separate duties between Human Resources and Payroll to achieve a higher level of risk mitigation.

*Human Resources had limited high risk areas*

The ISACA report listed only two high risk areas within Human Resources: 1) change employee HR benefits then process payroll without authorization, and 2) change master data and creating the remittance to a third party vendor. The first was categorized and reviewed as a Payroll item because the high risk is in the fraudulent disbursement of a payroll check. The second was determined as external because the risk was associated with a third party vendor and check disbursement which was covered under AP.

---

**REVENUE COLLECTIONS**



**Revenue Collections (RC)** is a division in ASD and is responsible for collecting City revenue generated from various city services. RC collects over \$97 million in revenue annually and is one of the most public-facing divisions of the City. RC has nine employees: a Manager, two Lead Account Specialists, and six Account Specialists.

Based on the matrix we developed in Exhibit 4, three conflicting tasks would need to be performed by at least three different employees for maximum separation of duties. Staffing levels are sufficient with nine employees in RC for effective separation of duties.



**EXHIBIT 4**  
**Revenue Collections**

Task No.	Task Description	Employee performing task		
		E1	E2	E3
<b>Revenue Collections</b>	<b>Operations</b>			
1	Cash application	X		
2	Bank reconciliation		X	
3	Maintain bank master data			X

 Employee should not perform task.  
 Employee should not perform task (not addressed on ISACA list).

**Mitigating Examples:**

If E1 can perform Task 1 & 2, they are able to steal cash by pocketing a cash payment and approving the deposit. A mitigating manual control would be to have a supervisory review and approval prior to bank deposit.

**SOURCE:** Auditor's analysis and summary of ISACA's "Best Practices to resolve Segregation of Duties conflicts in any ERP environment."

RC uses a revenue collection system external to SAP that is integrated to upload transactions into SAP. Due to the customer service and cash handling nature of RC, and the need for desk rotation, multiple employees are needed to fill the same role. Therefore, six of the nine employees in RC perform the same tasks and many of the processes are manual and paper-based. Under this current process, RC has well separated, administered, and mitigated the high-risk tasks.

Although Revenue Collections has a manual process in place to manage the risk of employees stealing cash, the control can be more effective. The current control is paper-based. It may be more effective to move to an automated reconciliation and reporting process.



## TREASURY

**Treasury** is a division of ASD and is responsible for managing and investing the City's funds and assets and facilitating debt financing. Treasury manages \$532 million of City cash and investments and has two employees: a Manager and a Senior Management Analyst.

Based on the matrix we developed in Exhibit 5, two conflicting tasks need to be performed by at least two different employees for adequate SoD in the high-risk areas. Staffing levels are sufficient with two employees in Treasury.

**EXHIBIT 5**  
**Treasury**

Task No.	Task Description	Employee performing task	
		E1	E2
<b>Treasury</b>	<b>Operations</b>		
1	Create/Change Treasury item	X	X
2	Confirm a Treasury Change	X	X

 Employee should not perform task.  
 Employee should not perform task (not addressed in ISACA).

Mitigating Examples:

If E1 can perform Task 1 & 2, they can create and approve a trade unsupervised. A mitigating manual control would be to require a trade to be approved by a supervisor or outside the department.

**SOURCE:** Auditor’s analysis and summary of ISACA’s “Best Practices to resolve Segregation of Duties conflicts in any ERP environment.”

The only high-risk conflicting task we reviewed in Treasury was the ability to create and confirm the processing of a stock trade. The process for the tasks is completed manually and is separated properly. However, automating some of these processes in the new ERP system, if possible, would achieve some efficiencies.

## UTILITIES

The City’s Utility’s Department (Utilities) operates and provides electric, gas, water, wastewater, and fiber optic services. Utilities performs many of the same high-risk duties as other divisions in the Administrative Services Department; however, the transactions are performed at a much less and more limited capacity. These duties include maintaining utility customer data, processing customer bills and payments, and collecting utility revenue.

Due to the limited transactions, we did not determine this to be a high-risk area. However, Utilities should follow the same separation of duties processes and practices established by the Administrative Services Department when performing the high-risk tasks.

The matrix in Exhibit 6 identifies the high-risk tasks performed by Utilities and the separation of duties needed. We encourage Utilities to continue implementing recommendations of previous audits to strengthen their processes, which will also strengthen the area of separation of duties.

### EXHIBIT 6 Utilities

Task No.	Task Description	Employee performing task						
		E1	E2	E3	E4	E5	E6	E7
<b>Utilities</b>	<b>Operations</b>							
1	Maintain customer data	X						
2	Process customer invoices		X					
3	Clear customer balance			X				
4	Maintain billing documents				X			
5	AP payments					X		
6	Process credit memos						X	
7	Cash application							X

Employee should not perform task.

Employee should not perform task (not addressed in ISACA).

#### Mitigating Examples:

If E3 can perform both 3 & 4, they can clear customer balances for personal gain. This could either be their own account or that of another customer. A mitigating manual control would be to require supervisory review and approval of changes to billing documents.

**SOURCE:** Auditor's analysis and summary of ISACA's "Best Practices to resolve Segregation of Duties conflicts in any ERP environment."

### INFORMATION TECHNOLOGY

The Information Technology (IT) Department is responsible for the overall operational duties for the ERP system, including development, maintenance, and administration. The matrix in Exhibit 7 identifies the high-risk tasks and the separation of duties needed in these areas.

### EXHIBIT 7 Information Technology

Task No.	Task Description	Employee performing task						
		E1	E2	E3	E4	E5	E6	E7
<b>Information Technology</b>	<b>Operations</b>							
1	Basis development	X						
2	Configuration		X					
3	Basis utilities	X						
4	Basis table maintenance			X				
5	Security administration				X			
6	Transport administration					X		
7	System administration						X	
8	Client administration							X

Employee should not perform task.

Employee should not perform task (not addressed in ISACA).

#### Mitigating Examples:

If E4 can perform Task 5 & 7, they are able to create a fictitious user and assign roles to that user in order to access roles for gain. A mitigating manual control would be to require supervisory approval for changes made to any user roles.

**SOURCE:** Auditor's analysis and summary of ISACA's "Best Practices to resolve Segregation of Duties conflicts in any ERP environment."

### High-Risk Areas

The IT Department has two distinct roles in the area of separation of duties: 1) within the IT Department as identified in the matrix, and 2) as support for all the work areas throughout the City. As with other work areas, separation of duties is tempered by the size of the IT staff; however, where separation of duties is not enforced, compensating controls are critical to reduce the risk.

Within the IT department, generally, the following separation of duties are key:

- Computer operators should be prohibited from making changes to programs and data.
- System development staff should not have physical access to computer rooms and not have update access to production data.
- Technical support staff should not have access to application programs, production data, or physical access to the computer room.

System access controls are an important part of IT's role in maintaining effective separation of duties. IT should be aware of and responsive to all the key components of access control, including authentication of who is given access, authorization toward what they are given access to do, an audit trail to identify what they have done, and administration to maintain privileges and manage administrators.

The IT department, responding to a prior SAP Security audit and a consultant's review of the City's separation of duties, has implemented positive changes to their separation of duties processes around access control. Their separation of duties policy has been updated to provide clarity regarding roles and responsibilities, for both IT staff and end users. A key, beneficial change is that the IT Service Desk is now responsible for resetting SAP passwords, which separated the SAP Basis Team's ability to have access to SAP user account creation and modification and password reset.

One area that should be reviewed for improvement during the ERP design and implementation period is the redefining of user access profile and roles. Defining user access by profiles and roles assignment is effective; however, how the profiles and roles are

defined and using the concept of least privilege are important to mitigating separation of duties. Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those absolutely required to perform routine, legitimate activities. Applied to people, least privilege means enforcing the minimal level of user rights, or lowest clearance level, that allows the user to perform his/her role. In the previous separation of duties examples, we identified areas where transactional access was given to users unnecessarily.

IT provides support to the various work areas. Our general review did not identify conflicts for concern; however, we would like to reiterate that where separation of duties is not possible due to limited staff, it is especially important for the end-user department to:

- Authorize transactions.
- Reconcile input/output and run-to-run cycles.
- Control changes to master files.
- Control resubmission of rejected transactions.
- Restrict access to assets such as cash, blank checks, negotiable documents and inventory.

---

## Recommendations

To help ensure that the City adopts best practices for separation of duties when transitioning to the City's new ERP system, we recommend that the City Manager direct all departments to consult with the Information Technology Department to adopt practices for ensuring separation of duties for high-risk conflicting tasks, based on the matrices in Finding 1, or develop mitigating controls where conflicts cannot be avoided. Specifically, we recommend that:

1. Administrative Services:
  - a) Transfer the task of entering Accounts Payable invoices to ASD Administration and either discontinue Account Payable's SAP access for entering invoices or, if not possible, create a procedure that can identify if/when an Accounts Payable invoice is entered by an Accounts Payable employee for supervisory review.
  - b) Have Payroll redesign the existing manual controls to mitigate against the high-risk areas of SoD conflict identified.
  - c) Share with Utilities all relevant SoD practices adopted, and Utilities practices should be consistent with that of ASD.
2. Information Technology revisit the design and definition of profiles and roles according to the concept of least privilege, where possible.

### APPENDIX 1 – City Manager’s Response

The City Manager has agreed to take the following actions in response to the audit recommendations in this report. The City Manager will report progress on implementation six months after the Council accepts the audit report, and every six months thereafter until all recommendations have been implemented.

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan	To be completed 6 months after Council acceptance and every 6 months thereafter until all recommendations are implemented	
			Current Status	Implementation Update and Expected Completion Date
<b>Finding 1: Implementing effective separation of duties and ensuring well-restricted user access controls for the new ERP system will decrease vulnerabilities and risks.</b>				
To help ensure that the City adopts best practices for separation of duties when transitioning to the City’s new ERP system, we recommend that the City Manager direct all departments to consult with the Information Technology Department to adopt practices for ensuring separation of duties for high-risk conflicting tasks, based on the matrices in Finding 1, or develop mitigating controls where conflicts cannot be avoided. Specifically, we recommend:				
1.a. Transfer the task of entering Accounts Payable invoices to ASD Administration and either discontinue Account Payable’s SAP access for entering invoices or, if not possible, create a procedure that can identify if/when an Accounts Payable invoice is entered by an Accounts Payable employee for supervisory review. 1.b. Have Payroll redesign the existing manual controls to mitigate against the high-risk areas of SoD conflict identified.	Administrative Services Department	Agree. Target Date: With new ERP. Corrective Action Plan: 1a. Explore the possibility of transferring the task of entering Accounts Payable invoices to ASD Administration. 1b. Explore having Payroll redesign the existing manual controls to mitigate against the high-risk areas of SoD conflict identified in the new ERP.		

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan	To be completed 6 months after Council acceptance and every 6 months thereafter until all recommendations are implemented	
			Current Status	Implementation Update and Expected Completion Date
1.c. Share with Utilities all relevant SoD practices adopted, and Utilities practices should be consistent with that of ASD.		1c. Share with Utilities all relevant SoD practices adopted, and Utilities practices should be consistent with that of ASD.		
2. Information Technology revisit the design and definition of profiles and roles according to the concept of least privilege, where possible.	Information Technology	<p>Agree.</p> <p>Target Date: June 30, 2020</p> <p>Corrective Action Plan: The plan is to review and modify as appropriate the approach to profiles and roles during the design and implementation phases of the new ERP system. If it makes sense timing wise, the new design will be incorporated back into the legacy system during the project. Determination of value and cost in retrofitting to the legacy system will be made during design.</p>		