Performance Audit:
Oracle Segregation of Duties

June 2016

City Auditor's Office

City of Atlanta

File #16.06

CITY OF ATLANTA
City Auditor's Office
Leslie Ward, City Auditor
404.330.6452

June 2016

Performance Audit:

Oracle Segregation of Duties

Why We Did This Audit

We undertook this audit to identify employees who have been granted Oracle system access that could allow them to perform conflicting business functions, increasing the risk of error or fraud.

What We Recommended

To resolve segregation of duties conflicts, the chief financial officer, the commissioner of human resources, and the chief procurement officer should:

- develop policies around segregation of duties
- request AIM (Atlanta Information Management) remove conflicting access not required for business purposes and document mitigating controls in cases where the access is necessary
- work with AIM to remove or re-design responsibilities with internal conflicts as part of the Oracle upgrade

The chief information officer should:

- assist departments to create mitigating controls and remove conflicting access
- require departments to justify a business need for conflicting access and assist in implementing controls to mitigate risks of these conflicts
- standardize responsibility naming conventions as part of the Oracle upgrade
- consider using task-based responsibilities to create greater transparency of security and to prevent future conflicts

For more information regarding this report, please contact us through our website at www.atlaudit.org.

What We Found

We identified 84 employees in 16 departments who had capability to perform incompatible business tasks within Oracle. About two-thirds of the conflicting task assignments related to payroll or purchasing. The remaining conflicts related to accounting or cash receipts. Overall, we identified 219 system access conflicts that could allow errors to go undetected or could allow an employee to perpetrate and conceal fraud.

About 60% of the conflicts resulted from the assignment of a single responsibility with an internal conflict. A responsibility in Oracle refers to a collection of menus and access rights allowing the execution of specific business transactions, such as adding a new employee, processing a vendor payment, changing an employee salary, and creating a purchase order. These single responsibility conflicts consisted mostly of super-user access granted to upper-level management.

Segregation of duties refers to the practice of dividing responsibilities among different employees so that no single employee has the ability to perpetrate and conceal a fraud. Ideally personnel performing any one of these functions — recording, approving, reconciling, or maintaining custody — would not also perform any of the other functions. Segregation of duties deters fraud because perpetrating a fraudulent act when incompatible duties are segregated requires collusion with another person.

We queried Oracle to test for 46 conflicting business task pairs related to purchasing, payroll, cash receipts, bank reconciliations and accounting entries as of November 2015. We found no instances of 24 of the 46 conflict pairs for which we queried.

Management Responses to Audit Recommendations

Summary of Management Responses		
Recommendation #1:	The chief financial officer, the commissioner of human resources, and the chief procurement officer should develop policies around segregation of duties.	
Response & Proposed Action:	• Finance and Human Resources are reviewing existing Oracle Financials responsibilities to identify and remove incompatible tasks from responsibility. • Procurement has a policy that users who have access to create purchase orders cannot also approve those orders, nor can they have responsibilities to receive against any orders.	**Agree**
Timeframe:	September 30th, 2016	
Recommendation #2:	The chief financial officer, the commissioner of human resources, and the chief procurement officer should request AIM remove conflicting access not required for business purposes. If business need exists for conflicting access, the commissioners should design and document a mitigating control, such as monitoring, to reduce the risk of the conflict.	
Response & Proposed Action:	• Finance is reviewing identified employees with incompatible Oracle Financials responsibilities and removing task/responsibilities or document need and/or risk control method. • AIM developed a responsibility report for the Department of Procurement to run to monitor all user responsibilities to prevent conflicting access from being granted and to identify conflicting access if it does exist. Super Users are not in any workflow hierarchies, therefore they cannot submit any requisitions or purchase orders that they create for approval. • Human Resources has requested AIM remove all access to payroll functions other than to view statements of earnings.	**Agree**
Timeframe:	September 30th, 2016	
Recommendation #3:	The chief financial officer, the commissioner of human resources, and the chief procurement officer should work with AIM to remove or re-design responsibilities with internal conflicts as part of the Oracle upgrade.	
Response & Proposed Action:	Finance proposes implementation and configuration of GRC as part of the Oracle R12 upgrade. The procurement consolidation, effective July 1st, 2016, will also address part of the responsibility access with the remainder being addressed in the Oracle R12 upgrade. The Department of Human Resources will also work with AIM in the upgrade to identify and remove unnecessary access.	**Agree**
Timeframe:	September/October 2017	
Recommendation #4:	The chief information officer should assist the chief financial officer, the commissioner of human resources, and the chief procurement officer in creating mitigating controls and removing unnecessary access creating conflicts.	
Response & Proposed Action:	The chief information officer will work with departments to remove existing conflicts by: • Requesting a list of users with conflicting responsibilities from DHR, DOP and DOF with authorization to remove same users • Removing users submitted by business	**Agree**

	• Updating business on actions taken The chief information officer will work with departments to create mitigation controls by: • Informing businesses of current responsibility request workflow which requires justification for each request • Obtaining the most current list of defined responsibility conflicts from Audit department • Upon receipt of requirements from DHR, DOP, DOF and Audit on the new responsibility approval workflow process, design and implement the approval solution within Oracle.	
Timeframe:	Q2 FY17- Dependent on when lists of users are received	
Recommendation #5:	The chief information officer should require the chief financial officer, the commissioner of human resources, and the chief procurement officer to justify a business reason for conflicting access and assist in the documenting and performance of mitigating controls to address the risk of conflicts required for business purpose.	
Response & Proposed Action:	• Inform business of existing self-service responsibility request workflow within Oracle which requires a business reason for responsibility assignment • Utilize new request workflow from Rec#4 to help the business identify conflicting responsibility at the time of their request • Continue to preserve transaction records for future audit of approved conflicting responsibilities	**Agree**
Timeframe:	Q2 FY17	
Recommendation #6:	The chief information officer should standardize responsibility naming conventions as part of the Oracle upgrade.	
Response & Proposed Action:	Include language in Scope of Work for Oracle upgrade to standardize responsibility naming conventions	**Agree**
Timeframe:	Q2 FY17	
Recommendation #7:	The chief information officer should consider the use of task-based responsibilities to create greater transparency of security and prevent future conflicts.	
Response & Proposed Action:	AIM will consider Including task based responsibilities (create, modify, approve) in SOW of Oracle upgrade after vetting the level of customization required for implementation	**Agree**
Timeframe:	Q2 FY17	

CITY OF ATLANTA

LESLIE WARD
City Auditor
lward1@atlantaga.gov

AMANDA NOBLE
Deputy City Auditor
anoble@atlantaga.gov

CITY AUDITOR'S OFFICE
68 MITCHELL STREET SW, SUITE 12100
ATLANTA, GEORGIA 30303-0312
http://www.atlaudit.org
(404) 330-6452
FAX: (404) 658-6077

AUDIT COMMITTEE
Marion Cameron, CPA, Chair
Cheryl Allen, PhD, CPA
Daniel Ebersole

June 29, 2016

Honorable Mayor and Members of the City Council:

We undertook this audit to identify employees who have been granted access in the city's Oracle system that could allow them to perform conflicting business functions, which increases the risk of error or fraud. Segregating incompatible duties reduces risk of error or fraud because no single individual can create and conceal an erroneous or fraudulent transaction. Perpetrating a fraudulent act when incompatible duties are segregated requires collusion with another person. We focused our review on function-level access assigned to employees through Oracle responsibilities. We timed the audit to allow management the opportunity of implementing corrective action prior to or concurrent with the planned Oracle upgrade.

The Audit Committee has reviewed this report and is releasing it in accordance with Article 2, Chapter 6 of the City Charter. We appreciate the courtesy and cooperation of city staff throughout the audit. The team for this project was Michael Schroth and Christopher Armstead.

Leslie Ward
City Auditor

Marion Cameron
Audit Committee Chair

Oracle Segregation of Duties

Table of Contents

Introduction 1

Background 1

Audit Objectives 2

Scope and Methodology 2

Findings and Analysis 5

Assignment of Incompatible Duties Increases Risk of Error and Fraud 5

Most Conflicts Related to Payroll or Purchasing 5

Recommendations 11

Appendices 13

Appendix A
Management Review and Response to Audit Recommendations 15

Appendix B
Number and Type of Conflicts by Department 19

Appendix C
List of Conflicts and Risks 21

List of Exhibits

Exhibit 1 Oracle Security Levels 2

Exhibit 2 Segregation of Duties Conflicts 6

Exhibit 3 Employee Conflicts by Department 7

Exhibit 4 Distribution of Conflicts by Employee 8

Exhibit 5 Single Responsibility Conflicts by Department 9

Introduction

We undertook this audit to identify employees who have been granted system access that could allow them to perform conflicting business functions, increasing the risk of error or fraud. We focused our review on function-level access assigned to employees through Oracle responsibilities. We timed the audit to allow management the opportunity of implementing corrective action prior to or concurrent with the planned Oracle upgrade.

Background

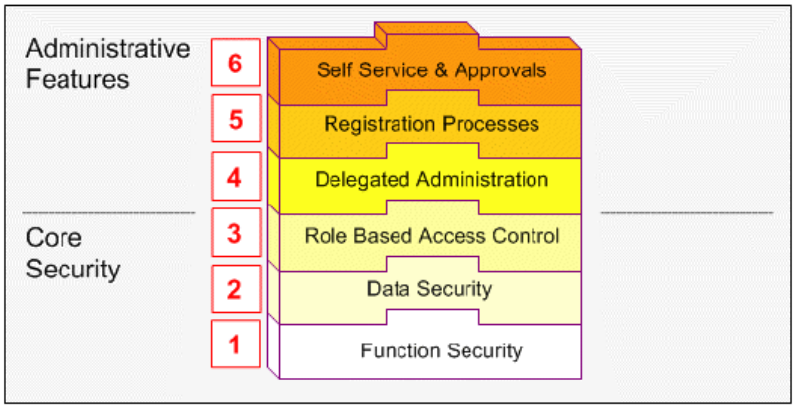
AIM (Atlanta Information Management) is responsible for assigning Oracle system access to employees based on the request and approval of individual departments. AIM assigns the access through responsibilities defined within Oracle. A responsibility in Oracle refers to a collection of menus and access rights allowing the execution of specific business transactions, such as adding a new employee, processing a vendor payment, changing an employee salary, and creating a purchase order.

Some of these business transactions, when combined with others, pose a risk to the city. Errors may go undetected, and the same individual may be able to perpetrate and conceal a fraud such as creating and paying a fictitious vendor or creating and paying a ghost employee. Segregation of duties refers to the practice of dividing responsibilities among different employees so that no single employee has the ability to perpetrate and conceal a fraud. Ideally personnel performing any one of these functions — recording, approving, reconciling, or maintaining custody — would not also perform any of the other functions. Segregation of duties deters fraud because perpetrating a fraudulent act when incompatible duties are segregated requires collusion with another person.

Oracle Release 11i has six separate levels of security, illustrated in Exhibit 1. Our audit focuses on the most basic level of function security, which controls user access to system functionality. Other levels of security may serve as mitigating controls for a particular conflict. For example, workflow approvals in level 6 may lessen the risk posed by a single employee capable of initiating a purchase order and receiving the same order. Data security controls, which restrict actions that can be performed on a specific data object,

such as deleting a record, may also offset risk posed by conflicting function security.

Exhibit 1 Oracle Security Levels



Source: Oracle User Management & Role Based Access Control with Oracle E-Business Suite Release 11i, October 2004

Audit Objectives

This report addresses the following objective:

- Identify segregation of duties conflicts within Oracle resulting from the assignment of a single responsibility as well as the assignment of multiple responsibilities.

Scope and Methodology

We conducted this audit in accordance with generally accepted government auditing standards. Our analysis focused on Oracle access rights in effect as of November 2015.

Our audit methods included:

- reviewing Oracle functional security
- interviewing department staff to validate our understanding of security
- reviewing responsibility matrices provided by department staff
- reviewing best practices for segregation of duties to identify conflicting business tasks

- mapping business tasks to specific functional access within Oracle
- querying Oracle to test for 46 conflict pairs related to purchasing, payroll, cash receipts, bank reconciliations and accounting entries
- identifying employees with one or more conflicts resulting from the assignment of multiple responsibilities and resulting from the assignment of one responsibility with inherent conflicts

Generally accepted government auditing 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.

Appendix C lists the 46 conflict pairs we tested for and the associated risk of each; no conflicts were found for the 24 shaded conflict pairs.

Findings and Analysis

Assignment of Incompatible Duties Increases Risk of Error and Fraud

We identified 84 employees in 16 departments who had capability to perform incompatible business tasks within Oracle. About two-thirds of the conflicting task assignments related to payroll or purchasing. The remaining conflicts related to accounting or cash receipts. Overall, we identified 219 system access conflicts that could allow errors to go undetected or an employee to perpetrate and conceal fraud. About 60% of the conflicts resulted from the assignment of a single responsibility with an internal conflict. These single responsibility conflicts consisted mostly of super-user access granted to upper-level management.

We recommend the chief financial officer, the chief procurement officer and the commissioner of human resources develop policies around segregation of duties to identify specific business tasks that should be separated. The chief information officer should develop a process to enforce the policies when assigning employee access. As part of the Oracle upgrade, the chief information officer should ensure that conflicting tasks are not included in a single responsibility. Also as part of the upgrade, the chief information officer should standardize responsibility naming conventions and consider the use of task-based responsibilities to create greater transparency in security and prevent future conflicts. To ensure the responsibilities will be easily understood by business and technical users alike, the names should make logical sense to both the business assigner/reviewer and the IT implementer so that it is clear what specific level of access is being granted.

Most Conflicts Related to Payroll or Purchasing

We identified 219 conflicts that could allow undetected errors or fraud. Conflicts related to payroll accounted for 43% of the conflicts we identified. These conflicts could allow an employee to make unauthorized changes to payroll and create fraudulent payments. Conflicts related to purchasing accounted for 23% of the conflicts we identified. These conflicts could allow employees to purchase goods for personal use with city funds, create a fraudulent invoice or create a fraudulent vendor. Conflicts related to accounting account for 18% of the conflicts we identified. These conflicts could allow an

employee to create journal entries in the wrong accounting period to conceal fraudulent activity. Conflicts related to cash receipt account for 15% of the conflicts. These conflicts could allow an employee to fraudulently change an invoice and change the payments made against the invoice. Exhibit 2 shows the total number of conflicts identified and the number of each conflict. Appendix B shows the number of each conflict by department.

Exhibit 2 Segregation of Duties Conflicts

Payroll Conflicts	Count
Payroll Maintenance v. Process Payroll	21
Maintain Employee Master Data v. Payroll Maintenance	17
Maintain Payroll Configuration v. Payroll Maintenance	15
Maintain Payroll Configuration v. Process Payroll	15
Maintain Employee Master Data v. Process Payroll	14
Maintain Employee Master Data v. Maintain Payroll Configuration	13
subtotal	95
Purchasing Conflicts	**Count**
Maintain Purchase Order v. Goods Receipts to PO	22
Process Vendor Invoices v. Goods Receipts to PO	15
Process Vendor Invoices v. AP Payments	5
Maintain Purchase Order v. Process Vendor Invoices	4
Vendor Master Maintenance v. Maintain Purchase Order	3
Maintain Asset Document v. Process Vendor Invoices	2
subtotal	51
Accounting Conflicts	**Count**
Enter Journals v. Open/Close Periods	13
Import Journals v. Open/Close Periods	9
Journal Authorization Limits v. Enter Journals	7
Journal Authorization Limits v. Import Journals	6
Enter Journals v. Process Customer Invoices	4
Enter Journals v. AP Payments	1
subtotal	40
Cash Receipts	**33**
Maintain Customer Master Data v. Process Customer Invoices	10
Vendor Master Maintenance v. Process Vendor Invoices	9
Maintain Customer Master Data v. Maintain Billing Documents	8
Bank Reconciliation v. Process Vendor Invoices	6
subtotal	33
Total	**219**

Source: Developed by audit staff based on data from Oracle as of November 18, 2015

We recommend the Department of Finance, the Department of Human Resources, and the Department of Procurement establish policies to identify the specific business tasks within their areas that should be separated.

We identified 84 employees with at least one conflict. The Department of Finance and the Department of Human Resources account for 50% of the employees with conflicts. Exhibit 3 shows the number of employees with conflicts by department.

Exhibit 3 Employee Conflicts by Department

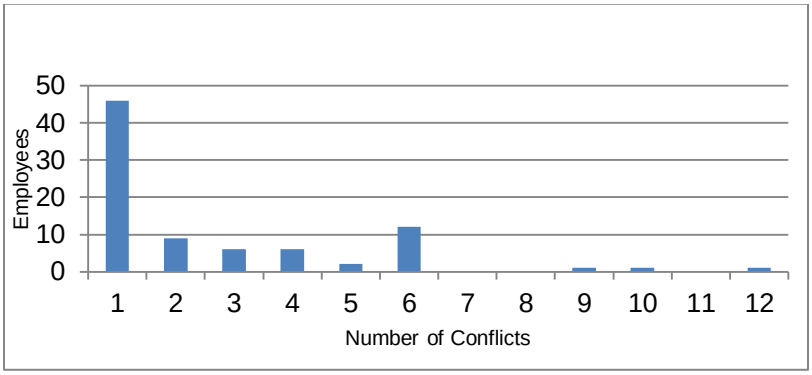
Department	Count	Percent
Finance	29	34.5%
Human Resources	13	15.5%
Aviation	10	11.9%
IT	5	6.0%
Parks	4	4.8%
Public Works	4	4.8%
Executive	3	3.6%
Watershed	3	3.6%
Procurement	3	3.6%
Planning	3	3.6%
City Council	2	2.4%
Municipal Court	1	1.2%
Solicitor	1	1.2%
Citizen Review Board	1	1.2%
Fire	1	1.2%
Police	1	1.2%
Law	0	0
Audit	0	0
Ethics	0	0
Corrections	0	0
Public Defender	0	0
Total	**84**	**100.0%**

Source: Developed by audit staff based on data from Oracle as of November 18, 2015

The number of conflicts per employees ranged from one to twelve. Forty-six of the employees had only one conflict; 15 employees had six or more conflicts. Exhibit 4 shows the breakdown of employees by number of conflicts.

We recommend the chief financial officer, the commissioner of human resources, and the chief procurement officer request the removal of one or more responsibilities causing the access conflict. If a business need exists for the conflict, we recommend the commissioners work with AIM to design and document a mitigating control, such as monitoring, to reduce the risk of the conflict.

Exhibit 4 Distribution of Conflicts by Employee



Source: Developed by audit staff based on data from Oracle as of November 18, 2015

Before granting department requests for conflicting access, the chief information officer should require the requesting department to justify the business reason for the access and should work with the department to develop and document a mitigating control.

We identified 14 responsibilities with internal conflicts. Of the 219 total conflicts, 127 result from the assignment of a single responsibility. These single responsibilities consist of upper management and super-users with broad access. We recommend that the chief financial officer, the commissioner of human resources, and the chief procurement officer request the removal of these responsibilities or work with AIM to remove the conflicts within the responsibility as part of the Oracle upgrade. If a business reason exists for a single conflicting responsibility, we recommend the department develop and document a mitigating control, such as monitoring, to reduce the risk presented by the conflicting access. Additionally, the chief information officer should standardize role naming conventions and consider the use of task-based responsibilities to create greater transparency in security and prevent future conflicts. Exhibit 5 shows the assignment of the single responsibility conflicts by department.

Exhibit 5 Single Responsibility Conflicts by Department

Department	Employees
Human Resources	12
Finance	19
Procurement	3
IT	4
Total	38

Source: Developed by audit staff based on data from Oracle as of November 18, 2015

Recommendations

To resolve segregation of duties conflicts, the chief financial officer, the commissioner of human resources, and the chief procurement officer should:

1. Develop policies around segregation of duties.

2. Request AIM remove conflicting access not required for business purposes. If business need exists for conflicting access, the commissioners should design and document a mitigating control, such as monitoring, to reduce the risk of the conflict.

3. Work with AIM to remove or re-design responsibilities with internal conflicts as part of the Oracle upgrade.

The chief information officer should:

4. Assist the chief financial officer, the commissioner of human resources, and the chief procurement officer in creating mitigating controls and removing unnecessary access creating conflicts.

5. Require the chief financial officer, the commissioner of human resources, and the chief procurement officer to justify a business reason for conflicting access and assist in the documenting and performance of mitigating controls to address the risk of conflicts required for business purpose.

6. Standardize responsibility naming conventions as part of the Oracle upgrade.

7. Consider the use of task-based responsibilities to create greater transparency of security and prevent future conflicts.

Appendices

Appendix A
Management Review and Response to Audit Recommendations

Report # 16.06	Report Title: Oracle Segregation of Duties	Date: July 2016
Recommendation Responses		
Rec. #1	The chief financial officer, the commissioner of human resources, and the chief procurement officer should develop policies around segregation of duties.	**Agree**
Finance **Proposed Action:**	Review existing Oracle Financials responsibilities for conflicting tasks and remove incompatible tasks from responsibility.	
Implementation Timeframe:	September 30th, 2016	
Comments:	DOF is already reviewing and taking steps to address segregation of duties controls for Oracle Financials responsibilities.	
Responsible Person:	Bertha Davis (Financial Systems Services)	
Human Resources **Proposed Action:**	Develop appropriate policies to address segregation of duty conflicts.	
Implementation Timeframe:	September 30, 2016	
Comments:	This policy is dependent upon fully understanding the segregation issues and identifying steps necessary to mitigate the issues.	
Responsible Person:	Catherine LeMay	
Procurement **Proposed Action:**	Current policies exist pertaining to segregation of duties. Users who have access to create Purchase Orders cannot also Approve those orders, nor can they have responsibilities to receive against any orders.	
Implementation Timeframe:		
Comments:		
Responsible Person:		
Rec. #2	The chief financial officer, the commissioner of human resources, and the chief procurement officer should request AIM remove conflicting access not required for business purposes. If business need exists for conflicting access, the commissioners should design and document a mitigating control, such as monitoring, to reduce the risk of the conflict.	**Agree**
Finance **Proposed Action:**	Review identified employees with incompatible Oracle Financials responsibilities and remove task/responsibilities or	

	document need and/or risk control method.
Implementation Timeframe:	September 30th, 2016
Comments:	DOF is already reviewing and taking steps to address segregation of duties controls for Oracle Finance responsibilities.
Responsible Person:	Bertha Davis (Financial Systems Services)
Human Resources	
Proposed Action:	A request has been sent to AIM to remove all access that is other than “VIEW” to “Statement of Earnings”.
Implementation Timeframe:	September 30, 2016
Comments:	This is requiring very detailed review to Screen level which is taking time.
Responsible Person:	Elaine Gooden
Procurement	
Proposed Action:	AIM developed a responsibility report for DOP to run to monitor all user responsibilities to prevent conflicting access from being granted and to identify conflicting access if it does exist. Super Users are not in any workflow hierarchies, therefore they cannot submit any Requisitions or Purchase Orders that they create for Approval.
Implementation Timeframe:	
Comments:	
Responsible Person:	

Rec. #	The chief financial officer, the commissioner of human resources, and the chief procurement officer should work with AIM to remove or re-design responsibilities with internal conflicts as part of the Oracle upgrade.	

Finance	
Proposed Action:	Implementation and configuration of GRC as part of the Oracle R12 upgrade
Implementation Timeframe:	September 2017
Comments:	Because complying with access control policies using manual processes is unreliable, DOF is asking AIM to purchase and implement Oracle Governance Risk and Compliance Management (GRC.) GRC will enable Finance to create automated access and segregation of duties controls and policies across all Oracle business applications. It will also incorporate advance controls to track changes to applications, set-up data, and monitor business transactions. With this suite of applications, control, monitoring, and reporting will be automated for compliance.
Responsible Person:	Alfonso Pinan (Financial Systems Services)

	Human Resources	
	Proposed Action:	Same as above where necessary additional “Responsibilities” will be removed
	Implementation Timeframe:	September 30, 2016
	Comments:	See above
	Responsible Person:	Elaine Gooden
	Procurement	
	Proposed Action:	Remove unnecessary and duplicate functions as well as Oracle responsibilities to minimize internal conflicts. The procurement consolidation, effective July 1st, 2016 will address part of the responsibility access with the remainder being addressed in the Oracle R12 upgrade.
	Implementation Timeframe:	October 2017
	Comments:	
	Responsible Person:	Kevin Floyd
Rec. #4	The chief information officer should assist the chief financial officer, the commissioner of human resources, and the chief procurement officer in creating mitigating controls and removing unnecessary access creating conflicts.	**Agree**
	Proposed Action:	The chief information officer will work with the chief financial officer, the commissioner of human resources and the chief procurement officer to create mitigation controls and remove access creating conflicts with the following actions: **Mitigating Controls for new responsibilities** • Inform business of current responsibility request workflow which requires justification for each request • Obtain most current list of defined responsibility conflicts from Audit department • Upon receipt of requirements from DHR, DOP, DOF and Audit on the new responsibility approval workflow process, design and implement the approval solution within Oracle **Remove Access creating conflicts** • Request a list of users with conflicting responsibilities from DHR, DOP and DOF with authorization to remove same users • Remove users submitted by business • Update business on actions taken
	Implementation Timeframe:	***Q2 FY17*** **for mitigating controls-** ***Dependent on when list of users are received; Q1 FY17*** **for removing access**
	Responsible Person:	CIO Samir Saini

Rec. #5	The chief information officer should require the chief financial officer, the commissioner of human resources, and the chief procurement officer to justify a business reason for conflicting access and assist in the documenting and performance of mitigating controls to address the risk of conflicts required for business purpose.	Agree
Proposed Action:	• Inform business of existing self-service responsibility request workflow within Oracle which requires a business reason for responsibility assignment • Utilize new request workflow from Rec#4 to help the business identify conflicting responsibility at the time of their request • Continue to preserve transaction records for future audit of approved conflicting responsibilities	
Implementation Timeframe:	***Q2 FY17*** **Dependent on completion of new self-service request workflow**	
Responsible Person:	CIO Samir Saini	
Rec. #6	The chief information officer should standardize responsibility naming conventions as part of the Oracle upgrade.	Agree
Proposed Action:	Include language in SOW for Oracle upgrade to standardize responsibility naming conventions	
Implementation Timeframe:	Q2 FY17	
Responsible Person:	CIO Samir Saini	
Rec. #7	The chief information officer should consider the use of task-based responsibilities to create greater transparency of security and prevent future conflicts.	
Proposed Action:	AIM will consider Including task based responsibilities (create, modify, approve) in SOW of Oracle upgrade after vetting the level of customization required for implementation	
Implementation Timeframe:	Q2 FY17	
Responsible Person:	CIO Samir Saini	

Appendix B
Number and Type of Conflicts by Department

Number of Employees by Department and Conflict	AFR	APD	CCN	CRB	DHR	DIT	DOA	DOF	DOP	DPW	DWM	EXE	JDA	PCD	PRC	SOL	Total	
Bank Reconciliation v. Process Vendor Invoices								6									6	2.7%
Enter Journals v. AP Payments								1									1	0.5%
Enter Journals v. Open/Close Periods								13									13	5.9%
Enter Journals v. Process Customer Invoices							1	3									4	1.8%
Import Journals v. Open/Close Periods								9									9	4.1%
Journal Authorization Limits v. Enter Journals								7									7	3.2%
Journal Authorization Limits v. Import Journals								6									6	2.7%
Maintain Asset Document v. Process Vendor Invoices								2									2	0.9%
Maintain Customer Master Data v. Maintain Billing Documents						1	1	6									8	3.7%
Maintain Customer Master Data v. Process Customer Invoices						1	4	5									10	4.6%
Maintain Payroll Configuration v. Payroll Maintenance					10	3		2									15	6.8%
Maintain Payroll Configuration v. Process Payroll					10	3		2									15	6.8%
Maintain Purchase Order v. Goods Receipts to PO		1	2	1		3	1	1	3	4		1	1	3		1	22	10.0%
Maintain Purchase Order v. Process Vendor Invoices								1		2	1						4	1.8%
Payroll Maintenance v. Process Payroll					10	3		8									21	9.6%
Process Vendor Invoices v. AP Payments								5									5	2.3%
Process Vendor Invoices v. Goods Receipts to PO	1						4	1		2	2	2			3		15	6.8%
Vendor Master Maintenance v. Maintain Purchase Order									2						1		3	1.4%
Vendor Master Maintenance v. Process Vendor Invoices								8							1		9	4.1%
Maintain Employee Master Data v. Maintain Payroll Configuration					10	3											13	5.9%
Maintain Employee Master Data v. Payroll Maintenance					13	3		1									17	7.8%
Maintain Employee Master Data v. Process Payroll					10	3		1									14	6.4%
Total	1	1	2	1	63	23	11	88	5	8	3	3	1	3	5	1	219	
	0.5%	0.5%	0.9%	0.5%	28.8%	10.5%	5.0%	40.2%	2.3%	3.7%	1.4%	1.4%	0.5%	1.4%	2.3%	0.5%		

Appendix C
List of Conflicts and Risks

Task1	Task2	Risk Description
Maintain Bank Master Data	AP Payments	Create a non bona-fide bank account and create a check from it
Maintain Asset Document	Process Vendor Invoices	Pay an invoice and hide it in an asset that would be depreciated over time
Maintain Asset Document	Goods Receipts to PO	Create an invoice and hide it in an asset that would be depreciated over time
Cash Application	Bank Reconciliation	Allows differences between cash deposited and cash collections posted to be covered up
Maintain Asset Master	Goods Receipts to PO	Create the asset and manipulate the receipt of the associated asset
Maintain Bank Master Data	Cash Application	Maintain a non bona-fide bank account and divert incoming payments to it
Vendor Master Maintenance	Process Vendor Invoices	Maintain a fictitious vendor and enter a vendor invoice for automatic payment
AP Payments	Vendor Master Maintenance	Maintain a fictitious vendor and create a payment to that vendor
Process Vendor Invoices	AP Payments	Enter fictitious vendor invoices and then render payment to the vendor
Maintain Purchase Order	Process Vendor Invoices	Purchase unauthorized items and initiate payment by invoicing
Maintain Purchase Order	Goods Receipts to PO	Enter fictitious purchase orders for personal use and accept the goods through goods receipt
Process Vendor Invoices	Goods Receipts to PO	Enter fictitious vendor invoices and accept the goods via goods receipt
Maintain Purchase Order	AP Payments	Enter a fictitious purchase order and enter the covering payment
Vendor Master Maintenance	Maintain Purchase Order	Create a fictitious vendor and initiate purchases to that vendor
Bank Reconciliation	Process Vendor Invoices	Can hide differences between bank payments and posted AP records
PO Approval	Goods Receipts to PO	Approve the purchase of unauthorized goods and hide the misuse of inventory by not fully receiving the order

Task1	Task2	Risk Description
PO Approval	AP Payments	Commit the company to fraudulent purchase contracts and initiate payment for unauthorized goods and services
PO Approval	Process Vendor Invoices	Release a non bona-fide purchase order and initiate payment for the order by entering invoices
PO Approval	Vendor Master Maintenance	Create a fictitious vendor or change existing vendor master data and approve purchases to this vendor
AP Payments	Bank Reconciliation	Risk of entering unauthorized payments and reconcile with the bank through the same person
Maintain Purchase Order	PO Approval	Where release strategies are utilized, the same user should not maintain the purchase order and release or approve it
Maintain Customer Master Data	Process Customer Invoices	Make an unauthorized change to the master record (payment terms, tolerance level) in favor of the customer and enter an inappropriate invoice
Cash Application	Maintain Billing Documents	Create a billing document for a customer and inappropriately post a payment from the same customer to conceal non-payment
Maintain Customer Master Data	AR Payments	Create a fictitious customer and initiate payment to the unauthorized customer
Cash Application	Maintain Customer Master Data	Risk of the same person entering changes to the Customer Master file and modifying the Cash Received for the customer
Maintain Customer Master Data	Process Customer Credit Memo	Maintain a customer master record and post a fraudulent payment against it
Maintain Customer Master Data	Maintain Billing Documents	User can create a fictitious customer and then issue invoices to the customer
Cash Application	Process Customer Invoices	User can create/change an invoice and enter/change payments against the invoice
Maintain Employee Master Data	Process Payroll	Modify payroll master data and then process payroll due to potential for fraudulent activity
Maintain Time Data	Process Payroll	Modify time data and process payroll resulting in fraudulent payments
Maintain Payroll Configuration	Process Payroll	Change configuration of payroll then process payroll resulting in fraudulent payments
Maintain Employee Master Data	Maintain Payroll Configuration	Change configuration of payroll then modify payroll master data resulting in fraudulent payments
Maintain Time Data	Payroll Maintenance	Enter false time data and perform payroll maintenance
Payroll Maintenance	Process Payroll	Change payroll and process payroll without proper authorization

Task1	Task2	Risk Description
Maintain Payroll Configuration	Payroll Maintenance	Change payroll configuration and perform maintenance on payroll settings
Maintain Time Data	Maintain Payroll Configuration	Modify payroll configuration and enter false time data
Maintain Employee Master Data	Maintain Time Data	Users may enter false time data and process payroll resulting in fraudulent payments
Maintain Employee Master Data	Payroll Maintenance	Users may maintain employee master data including pay rates and delete the payroll result
Process Customer Credit Memo	Maintain Billing Documents	User could create a fictitious credit memo and run billing due to prompt a payment to a customer, which could allow the customer to provide a kickback to the internal user
Enter Journals	Open/Close Periods	Create journal entries in wrong accounting periods to conceal fraudulent activity
Journal Authorization Limits	Enter Journals	Ability to circumvent journal authorization limits
Import Journals	Open/Close Periods	Create journal entries in wrong accounting periods to conceal fraudulent activity
Journal Authorization Limits	Import Journals	Ability to circumvent journal authorization limits
Enter Journals	Cash Application	Risk of person pocketing cash and adjusting journals to reflect a cash receipt
Enter Journals	AP Payments	Conceal fraudulent payments with journal entries
Enter Journals	Process Customer Invoices	Modify customer invoice and enter journal. Potential for fraudulent activity