CITY OF ATLANTA

LESLIE WARD
City Auditor
lward1@atlantaga.gov

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

TO: Sherman Bryant, Oracle ERP Program Director

FROM: Leslie Ward, City Auditor

DATE: January 19, 2007

SUBJECT: Ongoing Review of Oracle Implementation Phase 2: Review of the Finance, HRMS, and Purchasing Responsibility Matrices

In the November 2005 audit report *Pre-Implementation Review of the ERP System*, we recommended that employees should be prohibited from performing two or more of the following functions for a single type of transaction: record keeping (creating and maintaining department records), asset custody (access to or control of physical assets), authorization (reviewing and approving transactions), and reconciliation (assurance that transactions are proper). Separating these incompatible business functions is a control to ensure appropriate data entry and to prevent misuse of city resources.

In this review of the Oracle implementation process, our objective was to ensure duties within the Finance, HRMS, and Purchasing applications were properly segregated so that no one employee could perform incompatible functions. We reviewed each application's responsibility matrix document to help Enterprise Resource Planning (ERP) project teams and the steering committee manage implementation risks. We also examined Oracle application user guides, and performed interviews with city staff and consultants regarding Oracle functionality.

We concluded that the Finance and HRMS applications' responsibilities are properly segregated. We did not find a case where a responsibility had two or more incompatible functions. However, we found several areas of concern with the Purchasing application's responsibility matrices.

High level purchasing application responsibilities such as a Super User or manager have access to multiple incompatible functions. This excess of functions, for example, could allow a single employee to set themselves up as a city vendor, purchase items from themselves, collect payment from the city, and potentially write off the purchased items. Also, high level responsibilities as well as others have access to General Ledger set up functions. General

Ledger functions should be limited to only General Ledger users. Having users with multiple incompatible duties increases the risk of inaccurate or fraudulent transactions.

Controls over access to Oracle data and functions for all city employees can be strengthened by developing policies and procedures governing users' access to information. A procedure should be created to manage employee access when they change positions or leave the city. One approach would be to use Role Based Access Controls (RBAC), where job roles are defined to determine what applications a user needs and permissions they are granted. In this system, roles can be defined to include other roles. Also, policies should be created preventing users from accessing and updating their own personal information.

Because it is possible for an employee to be assigned to multiple responsibilities, there is still a risk that employees could be assigned to incompatible business functions. For example, employees who have access to responsibilities within the Projects and Grants application should not have access to the GL Property and Grants Coordinator responsibility functions within the GL application. In addition, the Bank Reconciliation responsibility in the Cash Management application should be limited because this responsibility has the ability to reconcile bank statements and make manual adjustments to bank statements. We strongly recommend the ERP Change Management Team to use the 2005 *Pre-Implementation Review of the ERP System* audit report as a guide when assigning employees to specific responsibilities. Relevant excerpts from the audit are attached.

A list of our recommendations is attached. We need written responses to these recommendations no later than **January 26**. We appreciate the opportunity to provide feedback on Phase 2 of the Oracle ERP Implementation and thank the project team for their courtesy and cooperation. We look forward to continuing this constructive relationship throughout the implementation process.

Please feel free to contact Gerald Schaefer at 404/330-6876 if you have questions or would like to discuss this further. You can reach me directly at 404/330-6804.

cc: Lynnette Young, Chief Operating Officer
Luz Borrero, Deputy Chief Operating Officer
Abe Kani, Chief Information Officer
Janice Davis, Chief Financial Officer
Adam Smith, Chief Procurement Officer
Benita C. Ransom, Commissioner of Human Resources
Elizabeth B. Chandler, City Attorney
Nate Holley, Oracle Project Manager
Delicia Nwadike, Finance Lead
Peggy Sangiorgi, Oracle Finance Lead
Keith Brooks, Procurement Lead
Raju Iyer, Oracle Procurement Lead
Felita Jones, Human Resources Lead
Kathleen Essig, Oracle Human Resources Lead
Audit Committee

Recommendations

1. The city should limit the system access of the PSP Super User and the PSP Manager. These responsibilities are able to complete the following tasks: create purchase orders, create vendors, receive and return items, and accrual write-offs. These four duties should be separated; otherwise, a single employee could set themselves up as a vendor, purchase items from the fictitious vendor they created, record fictitious items as received, and potentially write-off the items. In addition, the PSP Super User is able to maintain inventory documents and delete inventory items. These two record keeping functions over assets should be separate from receiving functions and from writing off accruals.

   Comments: The finance Department concurs with the recommendation. This represents a clear instance of conflicting responsibilities and violates a primary internal control tenet. The Department of Procurement is in agreement with the Auditor's recommendation as well. The "incompatible" functions were identified and discussed with the Auditor prior to the publication of this report. The "incompatible" functions for both the PSP Super User and the PSP Manager were identified and custom responsibilities will be created prior to SIT to assume these "incompatible" functions. For example, the PSP Super User will not have responsibility for Accounting, Accrual Write Offs, many Purchase Order related functions, Receiving, Flexfields, Tax, External Suppliers, Credit Cards, Contract Terms, Advanced Pricing Administration, Supply Base, Supplier Guest User Menu, Supplier Management, Workflow User and Advanced Pricing. Additionally, "incompatible" functions for the PSP were identified and scheduled for deletion prior to SIT. As stated by the PMO Office, the Responsibility Matrix is a "living document." It will undergo revisions throughout implementation. Per the SIT Strategy, the deadline to provide the technical resource, Germaine Ekamby, with custom responsibilities is February 7, 2007. A revised Responsibility Matrix will be created by January 28, 2007. Finally, the examples in Appendix 5 have been reviewed and will be incorporated in the updated Responsibility Matrix prior to the PMO deadline of February 7, 2007. The Department of Human Resources agrees and will comply with recommended Procurement, Financial and DIT processes as functions drill down to operating departments

2. The city should limit access to the General Ledger only to General Ledger users. The PSP Super User has access to the following General Ledger setup functions: GL Accounts, Open and Close Periods, and Define Credit Card GL Account Sets. Allowing the PSP Super User access to the General Ledger increases the chance for inaccurate or fraudulent transactions.

   Comments: The finance Department concurs with the recommendation. The Charter specifically requires that the CFO shall provide for the "administration of the financial systems of the city." This is a clear infringement on that requirement. The department of Procurement will present to the Department of Finance resources for review, comments and approval as it relates to the four applications (i.e., Purchasing, iProcurement and iSupplier, Property Management). The Department of Human Resources agrees and will comply with recommended Procurement, Financial and DIT processes as functions drill down to operating departments.

3. The Property Manager COA Super User and the Property Manager Administrator should not be able to both create vendors and authorize payments. Allowing these responsibilities access to both of these functions allows a single employee the ability to create a vendor and then pay the vendor without the involvement of another employee. Furthermore, the creation of vendors should be restricted to as few responsibilities as possible.

   Comments: The finance Department concurs with the recommendation. This represents a clear instance of conflicting responsibilities and violates a primary internal control tenet. The "Create Supplier" function will only be performed in the iSupplier Application. Again, this will be properly documented in SIT before February 7, 2007. The Department of Human Resources agrees and will comply with recommended Procurement, Financial and DIT processes as functions drill down to operating departments.

4. DIT should develop citywide policies and procedures for authorizing access to information resources and documenting such authorization. These policies should include procedures for terminating an employee's access to Oracle responsibilities when an employee leaves the city, and changing an employee's Oracle functional access to reflect their new duties when an employee changes positions.

   Comments: The Department of Information Technology (DIT) will develop an internal Standard Operating Procedure to provide/revoke access to information. However, the request for extending proper access or revoking an existing employee's access must be provided to DIT by the Departments of Human Resources, Procurement, and Finance. DIT does not know when a City employee leaves, is terminated, or has been transferred. This information must be submitted to DIT by the appropriate Departments in order to revoke a user's access. The finance Department concurs with the recommendation. The Department of Human Resources agrees and will comply with recommended Procurement, Financial and DIT processes as functions drill down to operating departments.

5. The city should implement Role Based Access Control (RBAC), which enables organizations to manage users based on job roles. Job roles can be defined to determine what applications as well as what data and functions within those applications a user can access. With RBAC, roles are hierarchical; so, roles can be defined that inherit other roles. Therefore, Oracle users can be assigned to a single role rather than multiple responsibilities. By leveraging the information about different groups already stored within Oracle applications, RBAC implementation has the ability to automatically assign roles, permissions, and responsibilities to users as they change positions or groups within the city. The benefits of implementing RBAC include: reduced costs in administering user access, streamlined setup and implementation of security policies, and user access based on an employee's job function. (In the November 2005 Pre-Implementation Review of the ERP System audit report, we recommended that Oracle user access should be based on roles).

   Comments: The finance Department concurs with the recommendation. The Department of Human Resources agrees and will comply with recommended Procurement, Financial and DIT processes as functions drill down to operating departments.

6. The city should prevent users from updating their own salary records in Oracle. An employee that has access to update employee's salaries in Oracle should not have access to update their own record.

   Comments: The finance Department concurs with the recommendation. The Department of Human Resources agrees that Oracle provides a HRMS security profile that prevents users from updating their own records, including salary. The Department will test this security during SIT.

APPENDIX 1

Excerpts from the 2005 *Pre-Implementation Review of the ERP System* audit report

Other modules

- Access to add, change, or delete the archive and purge functionality.
- The ability to input, change, cancel, or release credit memos.
- The ability to input, change, or cancel goods received.

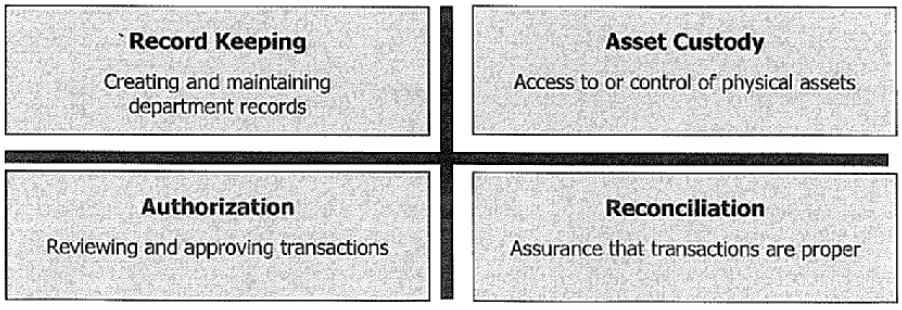
Lastly, access control processes should be in place to create, change, and terminate user access. These processes should be fully documented and continually refined throughout the ERP system implementation.

Incompatible business functions should be separated. Certain types of duties should be done by different employees as a control measure to ensure appropriate data entry and to prevent misuse of company resources. Consequently, incompatible business duties and responsibilities should be separated. This principal applies both to functions (i.e. what a person can do) and to information (i.e. what a person can see).

Incompatible duties assigned to one employee increase the risk of inaccurate or fraudulent transactions. To control this risk, no employee should be responsible for more than one of the following types of functions for a single type of transaction. (See Exhibit 4.)

EXHIBIT 4

FRAMEWORK FOR SEPARATING DUTIES



Source: Institute of Internal Auditors (Copyright 2004 Deloitte Development LLC)

Examples of the risks of combining these types of functions are shown below:

Record Keeping and Asset Custody: An employee is responsible for recording inventory and has access to the same inventory. A risk exists that the employee can steal city inventory.

Record Keeping and Authorization: An employee has access to set up a supplier in accounts payable and can authorize an invoice for payment. A risk exists that the employee can pay themselves with city funds.

Record Keeping and Reconciliation: An employee has the ability to write off accounts receivable and is responsible for reviewing all write-offs. A risk exists that the employee will write off debts that should not be.

Asset Custody and Authorization: An employee is responsible for a fleet of city vehicles and is responsible for performing a physical count of the vehicles at year end. A risk exists that the employee can steal a city-owned vehicle.

Asset Custody and Reconciliation: An employee collects cash generated from parking tickets and then is responsible for balancing his cash drawer at the end of the day. A risk exists that the employee can take the city's cash.

Authorization and Reconciliation: An employee has the authority to authorize a payment from a city account and has the responsibility of reconciling the bank account at the end of the month. A risk exists that the employee can misappropriate city funds.

A more detailed list of incompatible duties that should be separated is provided as Appendix 5 of this report.

Data Transferred to the ERP System Must be Accurate and Reliable

The city plans to transfer information from 43 different databases to the ERP system. These data currently reside in MARS-G, PeopleSoft, QuickBooks, Grants Management, and in various

APPENDIX 1 (continued)

Excerpts from the 2005 *Pre-Implementation Review of the ERP System* audit report

APPENDIX 5

EXAMPLES OF INCOMPATIBLE DUTIES

Separate this function	From this function
Ability to create and change purchase orders	Ability to process payments
Ability to create and change purchase orders	Ability to create or change vendors
Ability to maintain asset master data	Ability to run and review depreciation expense
Ability to create and change general ledger accounts	Ability to generate journal entries or other financial transactions
Ability to create and change deliveries	All other order processing activities
Ability to create and change purchase orders	Credit management activities
Ability to authorize payments	Ability to change bank information
Ability to create a purchase order	Ability to receive goods
Ability to create or change employee master data	Ability to process payroll
Ability to create and change customer master records	Ability to approve & process collections
Ability to maintain customer credit limits	Ability to approve & process collections
Ability to approve & process collections	Ability to issue goods
Ability to record revenues	Responsible for reconciling bank accounts
Ability to close accounts (period closings)	Ability to post journal entries