




# CITY OF ATLANTA

**LESLIE WARD**  
City Auditor  
[lward1@atlantaga.gov](mailto:lward1@atlantaga.gov)

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

**AUDIT COMMITTEE**  
Fred Williams, CPA, Chair  
Donald T. Penovi, CPA  
Cecelia Corbin Hunter  
Robert F. Ashurst, CPA  
Council President Lisa Borders

**TO:** Lynnette W. Young, Chief Operating Officer and ERP Steering Committee Chair

**FROM:** Leslie Ward 

**DATE:** February 28, 2007

**SUBJECT: Audit Trail Configuration in Oracle**

We are providing this memo to make recommendations on how the city should configure the audit trail and other security features in Oracle to prevent and detect unauthorized changes to data and settings. The audit trail keeps a history of changes to important data, recording what changed, who changed it, and when. While this information is critical for ensuring data integrity, organizations often fail to take advantage of auditing features due to perceived complexity and concern about reduced system performance. Properly configuring the audit functions, however, should not have a measurable performance impact on the Oracle applications or database.

Oracle is equipped with several different auditing features to monitor sign-on activity, transaction processing, and changes to database accounts or connections. Using each of these features together will provide a comprehensive and thorough audit trail. We provide detailed, technical recommendations to configure an audit trail for each of these features.<sup>1</sup>

## **Monitoring Sign-On Activity**

Oracle can audit and monitor user activity through the applications Sign-On Audit feature.

1. The Sign-On Audit level profile option allows an organization to select a level at which to audit users who sign on to Oracle applications. The profile option should be set to form at the site profile level, which provides the highest level of detail auditing. The default setting is none, which disables the Sign-On feature. The form option setting will allow the city to track all users, when they log in, what responsibilities or roles they use and what forms they access.

---

<sup>1</sup> We used the following sources as a basis of our recommendations: Oracle's Best Practices for Securing Oracle E-Business Suite version 3.0.4; Integrity's Guide to Auditing in Oracle Applications and Oracle Applications 11i Security Quick Reference; "Building an Audit Trail in an Oracle Applications Environment" OAUG Insight Spring 2006; Oracle's System Administrator's Guide – Security; Course Materials from : System Administrator Fundamentals, Building an Audit Trail in Oracle Applications Environment; and Auditing Oracle Applications Oracle Metalink Documents.

2. The Who: Display Type profile option of the "About This Record" window should be set to extended. The Sign-On data is automatically routed to the About This Record window and the extended setting captures the name of the user, date of the change made, name of the table changed, the name of the user that last changed the table, the user's operating system logon, and the computer that was used to make the change.
3. The Sign-On Audit feature can generate several reports detailing information gathered by Sign-On Audit. These reports track access signon, unsuccessful signon, responsibility usage, form usage, and concurrent request usage. These are standard Oracle reports and can be accessed through the system administrator responsibility. The city should run and periodically review these reports for unusual and suspicious activity. These reports will have to be purged from the system periodically. Purged records should be retained for at least 90 days.
4. Another feature that can be accomplished with Sign-On Audit is to provide users with a warning message if anyone has made an unsuccessful attempt to sign on with their username since their last sign-on. This feature should be activated by setting the Sign-On:Notification profile option to Yes.
5. The system administrator responsibility can use the monitor users window to monitor what users are doing online and in real time. The city should periodically use this feature to monitor usage.

### **Monitoring Application Transactions**

Oracle has the ability to build a complete audit trail of changes made to the database. Application level auditing works with the database to record information about a transaction as the application interacts with database tables. Any database table can be audited. By default, no tables are audited. We recommend that this function is enabled to audit tables, which control system security.

6. To enable this type of auditing the system profile option AuditTrail: Activate should be set to True. This feature should only be used for tables with a low volume of changes and not on tables that are accessed frequently or transactional tables. As a rule of thumb any tables that have more than 100 changes per hour should not be audited. We recommend auditing the following tables (at a minimum):

ALR\_ALERTS  
FND\_AUDIT\_COLUMNS  
FND\_AUDIT\_GROUPS  
FND\_AUDIT\_SCHEMAS  
FND\_AUDIT\_TABLES  
FND\_CONCURRENT\_PROGRAMS  
FND\_DATA\_GROUPS

FND\_DATA\_GROUPS\_UNITS  
FND\_ENABLED\_PLSQL  
FND\_FLEX\_VALIDATION  
FND\_FORM  
FND\_FORM\_FUNCTIONS  
FND\_GRANTS  
FND\_MENUS  
FND\_MENUS\_TL  
FND\_MENUS\_ENTRIES  
FND\_MENUS\_ENTRIES\_TL  
FND\_ORACLE\_USERID  
FND\_PROFILE\_OPTIONS  
FND\_PROFILE\_OPTION\_VALUES  
FND\_REQUEST\_GROUPS  
FND\_REQUEST\_GROUPS\_UNITS  
FND\_RESP\_FUNCTIONS  
FND\_USER  
FND\_USER\_RESP\_GROUPS  
FND\_RESPONSIBILITY

Audit trail records will have to be accessed through SQL and audit trail information should be purged from Oracle on a regular basis. Prior to purging, the audit trail should be disabled.

### **Monitoring Database Events**

Database auditing is useful for capturing information not directly logged or audited within Oracle. There are two risk factors, which should be monitored using database-level auditing – connections to the database and changes to Oracle database accounts, as changes to these accounts are rare and changes may indicate inappropriate or malicious activity. Monitoring and auditing database sessions provides useful information on database activity and is the only way to identify certain types of attacks, such as password guessing on an application schema. This type of auditing has minimal performance impact.

7. The city should enable database-level auditing. To implement this feature, the city should set the AUDIT\_TRAIL parameter in the init.ora file to DB, OS, or TRUE. The default value is FALSE. Through this feature the city should audit database connections (SQL> audit session) and database schema changes (SQL> audit user). This can be done using SQL commands.
8. The city should also enable these audit events: create database link, alter system, and system audit. These activities are not routinely executed and may indicate inappropriate activity. These events can also be audited by using SQL commands.

Page 4  
February 27, 2007  
Lynnette Young

9. The city should archive and purge the audit trail produced by these features on a regular basis, at least every 90 days. Also, the audit trail may contain confidential data and access to the audit trail should be restricted appropriately.

We look forward to continuing this constructive relationship throughout the implementation. Please feel free to contact Gerald Schaefer at 404/330-6876 if you have any questions or would like to discuss further. You can reach me directly at 404/330-6804.

cc: 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  
Sherman Bryant, ERP Program Director  
Jeff Telfare, Technical Lead  
Guvin Uzgil, Oracle Technical Lead  
Germain Ekamby, DBA  
Audit Committee