Absolute Technologies®

Leverage Your Investment in Oracle Applications™!

Case Study

Enhance SOX Controls Over IT Department's Activities in Oracle E-Business Suite Without Slowing Down User Support

Application Auditor

DB Transaction Auditing for SOX Compliance

Summary

Our Customer designs, manufactures, and sells digital video products and systems internationally. Oracle E-Business Suite is the primary financial business application.

For over a year during the Sarbanes-Oxley (SOX) audits, the Customer's auditors took exception to IT staff logging on in the production Oracle E-Business Suite environment in order to resolve problems reported by the business users. The IT staff logged on with Super User responsibilities and thus could do almost anything in the application. Eventually, the Customer's IT Director implemented administrative procedural controls that satisfied the auditors, but were burdensome for the IT staff, delayed responses to support requests, and provided no visibility on what the staff actually did in production.

The auditors told the Customer about software another client was using to correct a similar problem. The Customer installed Application Auditor (AA), which provided audit trails that detailed **what** the IT staff did in production, as well as **when** they did it. Now the Financial Business Analyst and IT System Administrator are able to match approved support requests to the audit trails to monitor the support activity.

Support response times and administrative workload are back where they used to be, and the new controls now satisfy both internal audit and the external auditing firm.

At the end of this case study we describe some of AA's current features and a January 2007 customer installation project. We show an example of an audit email notification and explain some Oracle E-Business Suite auditing considerations.

Audience:

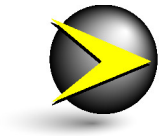
This case study is written for these readers:

IT Manager responsible for a) supporting the auditors in their review of the business application systems' controls, and b) demonstrating existence and effectiveness of IT environment controls.

Technical Evaluator responsible for a) assessing whether a product's technology is a fit with the company's architecture standards, b) deciding whether the product in fact works, and c) implementation if a subsequent purchase is made.

Audit or Business Evaluator responsible for assessing a) whether the product will deliver the capabilities to meet the current and future audit requirements, and b) is easy enough to use.

Internal Auditor or Controller responsible for a) documenting risks, b) developing mitigating controls over business processes, and c) reviewing the IT processes that support business processes, to ensure business objectives are met.



Absolute Technologies®

Leverage Your Investment in Oracle Applications™!

Contents

Customer's Business

2007 Revenue: $310M.
660 employees.
Fiscal Year End: 12/31.
Independent Auditor: PricewaterhouseCoopers (PWC).

The Customer designs, manufactures, and sells digital video products, systems, and software. They provide video delivery solutions to cable, satellite, telco, terrestrial and wireless operators around the world.

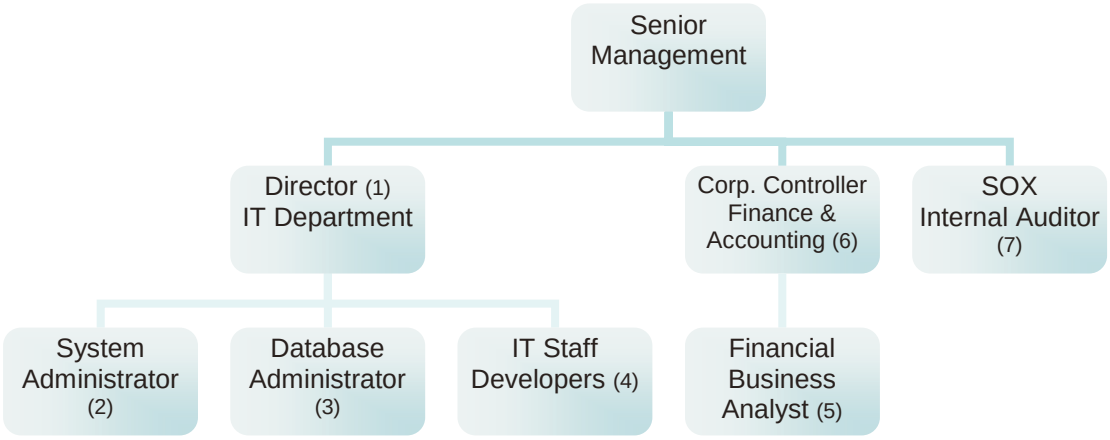
Oracle E-Business Suite

The Customer's primary business application is Oracle E-Business Suite. This application is within the scope of the financial audit and Section 404 of the Sarbanes-Oxley Act of 2002 (SOX). The IT Department is responsible for Oracle E-Business Suite, including IT access controls driven by the SOX audit.

Organizational Responsibilities

The IT Director (1) is responsible for Oracle E-Business Suite, including IT access controls driven by the SOX audit. The System Administrator (2) is responsible for granting access and privileges to IT Development & Support Staff to work in the production Oracle E-Business Suite environment. The Database Administrator (DBA) (3) takes care of the Oracle E-Business Suite solution architecture, performance, and day-to-day operations. There are about ten IT Staff (4) responsible for Oracle E-Business Suite perform developer and support functions (the Developers).

A Financial Business Analyst (5) in the Controller's Finance and Accounting organization (6) is responsible for monitoring the IT group's day-to-day production access, deciding whether transactions are authorized and proper, and detecting unauthorized transactions. An Internal Auditor (7) reviews the business and IT procedures.



PWC Audit Findings

Auditing firm PricewaterhouseCoopers (PWC) repeatedly noted that the Customer's IT Staff had unrestricted access to the production Oracle E-Business Suite application. The IT Staff logged in with Oracle Super User responsibilities in production, which allowed them to do almost anything in the application.

Since the access was not controlled or monitored, there were two risks: improper financial transactions and improper changes to application setups that define how financial transactions are processed and recorded.

Each Oracle module ships with a pre-configured super-user-like Responsibility that gives access to everything in the module, such as AP Super User or PO Super User.

Each IT staff person did both development and support work. They had a Production logon, to which was assigned all of these Super User Responsibilities for all the modules.

Initial Company Response

For over a year the Customer was able to convince PWC to allow this Super User access as an exception, because IT Staff needed to help authorized business users and sometimes fix transactions. They needed to be responsive and help users fast. At first, PWC was unable to offer suggestions that would satisfy the business control and retain the ability to respond quickly to support requests. They knew other companies faced a similar problem, so they allowed the practice.

The Customer tried to use Oracle Internal Controls Manager (ICM) to address this issue, but it didn't help with the access issues and it was not easy to use, so they stopped using it.

In February 2005, after the FY 2004 audit, PWC finally said the practice had to stop. The IT Development and Support Staff could no longer routinely have Super User access in Oracle. The Customer put in place administrative controls that were burdensome for the IT Staff.

Administrative Control Over IT Support Access to Production

The IT Department revoked the Oracle Super User responsibilities assigned to IT Development and Support Staff's logons.

When an Oracle business user needed help, they logged a trouble ticket or sent an email to IT, both of which were saved. They might discover that a sales order was not moving through the system and ask IT to get it "un-stuck." There was a separate form for Setup change requests. The System Administrator would assign the relevant modules' Super User Responsibilities to the IT Support person who was going to investigate and fix the problem, or change the Setup. When the work was complete, the System Administrator had to revoke those Responsibilities.

The System Administrator sometimes had to grant herself access, make changes, revoke that access, and report it to Finance.

She had to keep detailed logs in order to tie the original request email to the granting and revoking of Super User Responsibilities to IT Staff. The System Administrator provided the logs to a financial analyst in the Finance Department who would review and approve the support events.

This procedure ensured that there were logs of **when** the support person had Super User access in production, but there was no way to determine **what** was actually done.

These administrative steps were a lot of work. The procedure required them to record Support access that was of interest to the SOX auditors, but also access that was not. They had to log, document, and review situations when the IT Support person did not make any changes in the application, as well as those changes without financial impact.

Impact of Administrative Process

This control process was slow for the System Administrator, the IT Support team, and the business users. The System Administrator was spending too much time on administrative controls over IT access to the Oracle production application. The process added elapsed time to the resolution of the business user's support request.

There was **no record of what the IT Support person actually did** in the application. The control produced little tangible benefit and was superficial.

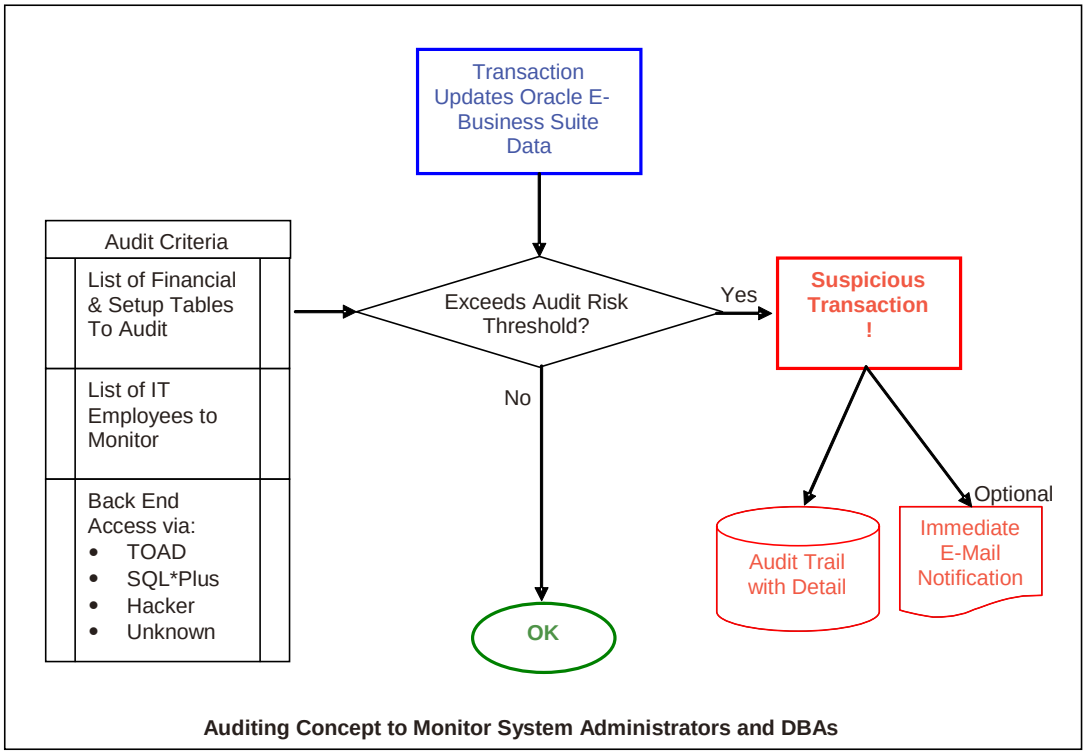
Required Capabilities

The requirements were to ensure that any System Administrator or DBA work was approved and unauthorized access could be detected.

The main objectives were:

- Maintain records of IT access to production.
- Allow both the System Administrator and the Business Analyst in Finance to tie the support request to the IT Support actions in production.
- Eliminate the System Administrator as a gating factor in responding to a support request.
- Retain IT Support's ability to get to any screen or function in Oracle necessary to diagnose or solve the reported problem.
- Detect if the Support person (or anyone else) bypassed the Oracle E-Business Suite interface and changed any data through the 'back door,' using SQL tools.

If the IT Director and the System Administrator could do those things, then they would be able to show that IT access control was working, PWC would clear the deficiency, and they could speed up the support process.



Auditing Concept to Monitor System Administrators and DBAs

The illustration above is a simplified version of the logic behind the requirements.

Decision Process

In late spring 2005, the PWC audit team met with the IT Director and his team. They told the IT Director about Silicon Image, another PWC audit client that was using Application Auditor (AA) to resolve a similar access control problem.

The IT Director, the System Administrator, and the DBA took a close look at AA. They concluded that with AA they could create an informative audit trail of developer activities in production, eliminating the need for the manual process, and thus regain the ability to quickly and effectively respond to support requests.

The System Administrator presented her plan to use AA to both PWC and Finance. PWC agreed AA would satisfy the controls they wanted the Customer to have. Finance also thought AA would meet the control objectives. They were not concerned with how IT implemented the business control, so they concurred with IT's decision to deploy AA.

Transition Project

The team set September 30, 2005 as the go-live goal for AA.

Absolute Technologies assisted the DBA with the installation and configuration of AA. After installing the product in the DEV instance, the DBA spent approximately 25% of his time, two weeks spread out over two months, configuring and testing AA audits. He had business users in the testing environment enter transactions to prove all the audit configurations were working. The System Administrator also helped with the testing, on and off for about two weeks. They concluded the product worked; it was generating audit trail records according to the user defined audit configurations with no noticeable impact on overall system performance.

Another AA Customer, Zoran Corporation, installed AA in production in two elapsed weeks, start to finish.

They installed AA in production on schedule.

PROJECT TIMETABLE

- 2005 June: Decision to buy AA.
- August 1: Project Kickoff.
- Sept 30: Production Go-Live.
- December: successful SOX Audit.
- 2006 August: Application Auditor sustaining Operations.

No Performance Impact

The DBA needed to be confident that AA would not degrade system performance. AA uses Oracle Database trigger technology. Using triggers in a production environment adds an additional layer of processing to transactions performed against the triggering table, and theoretically could impact database response times and decrease user satisfaction. He carefully observed response times during the active testing and the overall time AA was in the user testing environment prior to going into production. He saw no evidence of performance degradation due to AA and the use of triggers.

There was no performance degradation when they went into production, either. Customers have evaluated AA's optimized approach to trigger creation for ten years in production database operations without raising concerns.

The Customer installed all of AA's 30 seeded audit configurations in 2005. AA has 90 in 2008.

Solution – IT Perspective

The IT Director, the System Administrator, and the DBA use AA's seeded audit configurations. The approach is risk-based. These configurations detect very specific transactions in Oracle and create corresponding audit trail records. The transactions were selected because they:

- impact financial business records,
- impact application configuration setups that control how financial records are processed, or
- grant access to use financial transactions.

With the members of the IT staff assigned to an AA 'watch group' embedded in the audit configurations, AA only writes an audit trail record when any of the IT staff execute any of the audited transactions, while ignoring when business users execute financial transactions.

The audit trail record doesn't flood the auditor with an excessive number of fields. It includes before and after values for the desired financial

fields, other reference fields, session details and lookups from other tables as required. With this record content, an auditor doesn't need to hunt for other relevant data in order to decide whether the transaction should be approved.

Solution – Finance Perspective

The Financial Business Analyst was hired during the AA implementation. She is the final approver of IT's access to production. She needs to know that there was a valid request when an IT Staff person worked in the production application. Did the IT Staff person actually update any records? Are those records related to the request? Were any other records updated, unrelated to the request? The System Administrator monitors the work too, but the Financial Analyst is the final approver.

Every morning, the Financial Analyst uses AA's Administrator role to check that there have been no changes in any of AA's audit configurations that would compromise the integrity of the audit trails. With this secure capability, she can detect whether the System Administrator, the DBA, or anyone else has tampered with AA's database code or configurations of the audit trails.

Requests for IT Support in production come from one of the three sources: a Remedy helpdesk ticket, a setup request form, or an email. They go to the IT Support Team, with copies to the System Administrator and the Financial Analyst. The IT Support Team responds quickly. The System Administrator monitors the audit file periodically during the day via an Oracle Discoverer view, and sees the audit trail record of the support work. Since she is copied on the requests, she matches the request to the audit trail record, to prepare the documentation for the Financial Analyst's weekly review.

The Financial Analyst uses a report in Discoverer once a week to see all the audit trail records of the IT Support Staff activity in Production. There are on average 300 records per week and about 10% have a financial impact. If the Financial Analyst finds that the audit records on the report have proper authorization backup, she approves them. This process takes her about 45 minutes per week.

Once a quarter, the Internal Auditor reviews the Financial Analyst's work. He's also satisfied that the new access controls on the IT Staff are effective.

SOX and Accounting Controls

The Customer has approximately 40 business controls over the Oracle business application. The System Administrator said that with the 30 audit trail configurations, AA plays a contributing role in 70% of the controls.

AA captures an audit trail of the System Administrator's system administration transactions, such as end-dating a user, assigning responsibilities, or modifying responsibility records. The Financial Analyst is able to review and approve this activity.

The Customer is satisfied with the initial 30 seeded configurations. Since PWC didn't ask for any additional audit trails, there was no need to create and configure any Customer-specific audit trails.

Another AA customer told Absolute Technologies it takes about an hour to configure, test, and put into production a custom audit trail.

Results

The Developers regained Super User access in production to carry out their Support role. Now they can respond more quickly to user support requests, like they could before the access controls were put in place.

The Financial Analyst is satisfied that the process for requesting, authorizing, and executing the IT Support Staff work is in place and effective. She knows that the System Administrator is checking activity throughout the week, and the two of them would quickly detect unauthorized activity. There is hard copy documentation. In 45 minutes each week the Financial Analyst reviews and approves the approximately 300 audited transactions including the documentation for the 10% that require a formal request. The System Administrator spends far less time than in the three quarters prior to the implementation of these controls.

According to the Customer, PWC is satisfied with the IT Developers' production access exposure. They know the Customer:

- Would find out immediately if a Developer misused production Super User access to create unauthorized financial transactions or data, either by:
  - going into production without the proper support request, or
  - expanding the scope of an authorized support request beyond what the user needed.
- Knows when Developers actually change records in production.
- Can trace all the Developers' financially impacting transactions to see details of what they actually do in production.

The DBA said AA is very stable and he doesn't have to worry about it. AA doesn't increase his day-to-day workload. There is no noticeable impact on application performance.

Application Auditor Release 2.25

AA's current release includes:

- AA now has a built-in mechanism to define and manage **"User Watch Lists"** for the Oracle E-Business Suite, to simplify monitoring System Administrator and DBA activity. This feature is also useful to monitor activities of outsourced or remote accounting services staff.
- There is a set of **90 seeded audit configurations** for the Oracle E-Business Suite designed to identify SOX compliance issues. The set provides more flexibility to meet stricter audit requirements without additional investment.
- The Conflict Manager for the Oracle E-Business Suite provides a way to define, report and detect Segregation Of Duties (SOD) conflicts associated with Users, Roles, Responsibilities, Menus, Functions, and Forms.
- If the DBA tries to tamper with any objects in the AA schemas or to change the AA user's password, AA will **prevent** the changes, **create** an audit trail record, and **notify** a designated IT or business security person.
- AA audit configurations now support **prevention**, audit, and **alert** of any change transacted against defined table columns or any DDL operation across defined schemas.

Configurable email alert contains all relevant information from the audit trail.

New security option protects AA from DBA level data manipulation, which maintains the integrity of the audit mechanisms and trail, and creates an effective segregation of access between the DBA and the AA user.

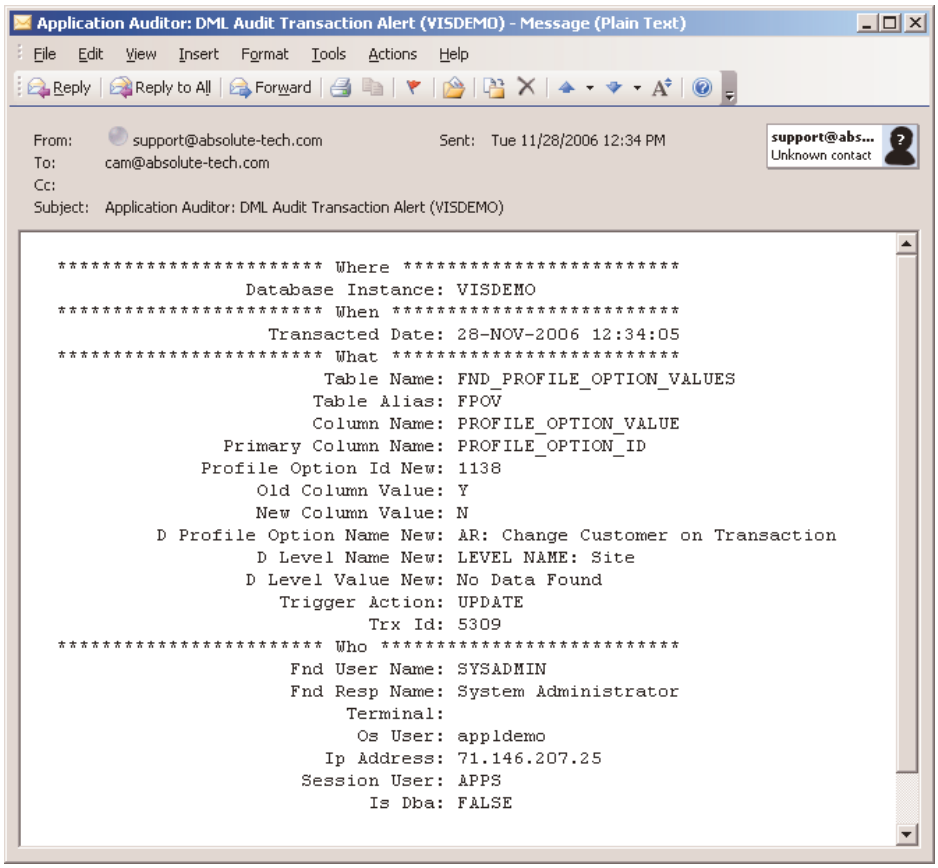
January 2007 Customer Installation of Release 2.25

Another Absolute Technologies customer started their Application Auditor deployment project in early 2007. The lead analyst and system administrator prepared the environment with the required directories, software files, logon authorizations, and environment variables. Software installation then took the lead analyst about 4 hours.

Absolute Technologies provided some remote trouble-shooting assistance, validated the installation, and trained the analyst on the use of all product screens and functions. Absolute also provided a site-specific script to activate a watch list of selected users for all audits. Our observation is that the **lead analyst and Absolute each devoted about 6 hours** over the course of two weeks. This customer has trained another analyst who has primary responsibility for AA operations for IT. They adjusted some of the seeded audit configurations and tested AA over the course of a week. Then they went live with AA before the end of March.

Example Audit Transaction Alert

Application Auditor allows you to create an email alert, with all relevant information from an audit trail record. This is what they look like.



The alert lists the Oracle E-Business Suite (FND) user name, and the active responsibility. If the transaction had been executed via the “back door” using direct SQL commands or tools, then these Application logon specific details would not be available, but details like Terminal, IP Address, Session User and OS user would be provided to identify the transacting user.

The audit trail also includes the table name and various fields with before and after values. You can also have Application Auditor look up useful information from foreign key records at the time the audit trail is created. That saves an auditor time when reviewing the audit trail, plus it captures the foreign record’s information at the time of the audited event, which is important since the foreign record could change before the auditor reviews the audit trail.

Supplement: Auditing Considerations for Oracle E-Business Suite

Oracle SQL Audit

Standard SQL Audit in Oracle, allows you to audit at three levels: statement, privilege, and object. This will create an audit trail record of the SQL statement that was executed. It will not provide the impact to rows and columns of data in the database as a result of running the statement. For that, you would need to employ table based database triggers, Fine Grained Auditing or Log Miner.

SYS User and SYSDBA

Oracle 9i/10g data dictionary tables are owned by the SYS user/schema, and can only be modified by the SYS user. All other database users, even SYSTEM or USERS granted the DBA role are limited to read-only access.

In 9i/10g, the only way to login to SYS is to have been granted the SYSDBA privilege. SYSDBA has complete control of the SYS.AUD$ table used to store the audit trail captured by SQL Audit, as well as the capability to execute or disable any audit commands.

Thus, if your objective is to audit your DBA logged on as SYSDBA, this approach is easily overcome by the very same DBA you are trying to audit. All the control is in his/her hands; it won't pass an SOD test.

Secure Audit of SYS User

However, Oracle 9i/10g does provide an initialization parameter called AUDIT_SYS_OPERATIONS. When set to TRUE, all "audit records for SYS are written to the operating system file that contains the audit trail, and not to SYS.AUD$. All SYS-issued SQL statements are audited indiscriminately and regardless of the setting of the AUDIT_TRAIL initialization parameter," (Oracle 9i Database Administration Guide).

In order to protect and secure the audit trail with respect to SYS, you must use this approach and secure from the DBA the OS directory in which these files are written.

Audit Users or Tables

Whether it is better to audit USERS rather than TABLES depends on the type of application you are running on your Oracle Database. If you are running Oracle E-Business Suite, then most of your database activity will come from the APPS user, since anyone logging into Oracle E-Business Suite logs onto the database as APPS. You cannot identify which actual user (person) is changing or executing what. On the other hand, some applications generate individual DB users for each actual person/login account.

Generating an audit record that records the Oracle E-Business Suite User and active Responsibility detail is possible using table-based database triggers, or Log Miner, or both. There are a few third party software vendors that provide automated solutions that include such functionality.

Application-Level Audit

Ultimately, there is no distinction between auditing at the application level and database level. For the audit trail to be accurate, both require that database transactions be audited. In other words, all auditing is database-level auditing.

There is a significant distinction between auditing those transactions that result from the use of the application versus those that result from IT or DBA staff activity using SQL tools. Most of the former will not require auditing, since the application is in control. All of the latter activity should be audited.

DML and DDL Audits

Another important distinction when approaching database auditing is DML (data manipulation) versus DDL (data definition). DML pertains to those transactions that directly impact data in

tables: inserts, updates and deletes. DDL pertains to statements executed that impact the definition of DB objects, those that create, alter, or drop tables, views, procedures, users, etc.. DDL statements include those that are operational, impacting table sizes and storage, as well as those that change the definitions or formats of business data.

FGA

Fine Grained Auditing (FGA) is a mechanism designed to audit SELECT access to tables at the record and column level. It is deployed and maintained by a DBA using packaged Oracle procedures from the SQL command line. This may be an important component of your audit strategy if you must maintain an audit trail of users who actually view sensitive or restricted data. However, it does require DBA level expertise to deploy and maintain, and has a performance impact that must be scrutinized and optimized.

Absolute Technologies, Inc., helps companies leverage their Oracle Applications investment through its line of products and solutions. Absolute provides software, professional services and support to assist customers with critical business functionality in particular under-developed areas of the Oracle Applications domain.

Founded in 1997, Absolute's commitment to affordable and innovative solutions for Oracle Applications customers is one of the main reasons why our customer base continues to expand year after year. Absolute solutions accommodate virtually any size company utilizing Oracle Applications. Our customers represent businesses in Manufacturing, Financial, Distribution, High-Tech and Internet industries.