Application Auditor
And
SOD Violations Manager

Frequently Asked Questions

Phone/Fax 888-270-3012

555 Bryant Street #440
Palo Alto, CA 94301

www.absolute-tech.com
support@absolute-tech.com

Aa

Application Auditor

by Absolute Technologies, Inc.

Here are frequently asked questions about Application Auditor and SOD Violations Manager. You'll find the answers on the pages that follow.

1. What are the two products, Application Auditor (AA) and SOD Violation Manager (SOD VM)? How are they related?
2. What's the difference between static and dynamic SOD controls? Do I need both?
3. Do I need two function conflict lists, one for static SOD and one for dynamic SOD?
4. What are the user watch lists in the E-Business Suite Extensions for SOD?
5. Can I start with SOD VM, and upgrade later to more of the Application Auditor functionality or extensions?
6. What if I don't want the 1200 SOD function conflicts you provide, but I do want SOD VM or the E-Business Suite Extensions for SOD?
7. Do you provide SOD and access reporting?
8. What if I want some users to have access to a pair of functions, but for everyone else it would be an SOD conflict and should be reported?
9. What if there's a sensitive function I want only a select few to have access to, and it's not necessarily in conflict with any other function?
10. What's the usual SOD compliance process with SOD VM or AA?
11. Tell me more about Application Auditor.
12. How about some details on the audit trails themselves?
13. Can I populate an audit trail destination table other than the Audit Table provided?
14. Can I use Application Auditor to track changes to EBS configurations and setups, and to master data like Customer or Product?
15. Does Application Auditor support E-Business Suite R12?
16. I'm going to upgrade from 11i to R12 soon. Can I deploy Application Auditor before the upgrade, and if I do, are there any special considerations?
17. Will I still be able to apply E-Business Suite patches and patch families, and add new modules?
18. What happens if something does go wrong and I need to call Oracle Support?
19. Has Oracle certified your Application Auditor software to operate properly with the E-Business Suite?
20. How will I know if Application Auditor works in my E-Business Suite environment?
21. It sounds too easy, what else is involved?
22. What training do you provide?
23. Will you help me design and deploy my SOX and SOD controls?
24. How long does it take to implement and deploy Application Auditor? How about SOD VM?
25. Who needs to be involved with installing and running Application Auditor?
26. Do you use database triggers to audit the tables?
27. Do I have to re-key the audit configurations when I am ready to transport them to Production?
28. Can I disable or turn off an active audit?
29. What if I get an error?
30. Do you provide a purge mechanism for the audit table?
31. Are there any restrictions to what you can audit?
32. What versions of the Oracle database are supported?
33. Is AA integrated for use with Oracle E-Business Suite?
34. Our Oracle E-Business Suite environment is hosted by an outside service. Can I still use AA or SOD VM?
35. Why not use Oracle Application's audit trail feature?
36. Why not use Oracle Governance, Risk, and Compliance Controls Suite?
37. How can I learn more or get the software?

Q-1. What are the two products, Application Auditor (AA) and SOD Violation Manager (SOD VM)? How are they related?

A. Application Auditor is both the underlying software engine and a family name for the engine and several configurable components. The complete AA functionality supports a range of controls for Oracle E-Business Suite and Oracle Database customers. SOD Violation Manager is a subset of the AA functionality, offered by subscription for customers who have narrow E-Business Suite segregation of duties controls requirements. Here are the different components.

Component	Description
Application Auditor	***Core Product*** Application Auditor for Oracle Database (9i, 10g, 11g) enables end users to capture and report changes to selected data elements in the database by defining and activating audit configurations via online forms. AA can audit DML [record level inserts, updates and deletes] and DDL [create, alter, drop, grant and revoke object] changes, as well as database (DB) logons. By operating at the DB level, AA can automate application and DB level controls. Please refer to the AA product data sheet for more information.
SOX Pack	***Application Auditor add-on module*** Ninety (90) seeded Oracle E-Business Suite (11i, R12) audits for master data, configuration data and application transactions with financial impact, designed to identify SOX Compliance issues. These are loaded directly into Application Auditor.
E-Business Suite Extensions for SOD	***Application Auditor add-on module*** These extensions provide additional functionality, and seeded data content, specifically to support both static and dynamic Segregation of Duties controls in E-Business Suite. ▪ SOD Violations Manager, to define, maintain, and identify Segregation of Duties conflicts associated with Oracle E-Business Suite 11i or R12 user access methods via Responsibilities, Menus, Forms and Functions. ▪ Twelve hundred (1,200) seeded Oracle E-Business Suite function conflicts across 21 modules ▪ Reports for function assignment conflicts and user access menu hierarchies. ▪ User Watch Lists, to define and maintain sets of application users to include or exclude from audit.
SOD Violations Manager	***Subscription for Application Auditor Static SOD functionality*** SOD Violations Manager (VM) is packaged as a completely stand

Component	**Description**
	alone product, and supports static SOD controls in EBS. The same functionality is included in AA with the E-Business Suite Extensions for SOD. ▪ SOD Violations Manager. ▪ Twelve hundred (1,200) seeded Oracle E-Business Suite function conflicts across 21 modules. ▪ Reports for function assignment conflicts and user access menu hierarchies.

Q-2. What's the difference between static and dynamic SOD controls? Do I need both?

A. The key distinction between the complementary static and dynamic SOD controls is that the static control interrogates the database periodically at the user's discretion to determine the state of the data at that moment. Whereas the dynamic control continuously monitors the database for data that is not aligned with your control policies and automatically notifies the user when policies are violated. For example, a report which provides a snapshot of who has access to what, and whether they have access to conflicting functions at the time of report submission, is an example of the static control. The dynamic control allows you to immediately detect application changes that create an access path to one or more conflicting functions, and respond to the conflicts in real time.

Whether you need one or the other or both should depend on your risk assessment and the corresponding need to mitigate that risk with automated controls. Consider what each tells you:

- Static SOD reports and analysis tell you who has potential to perform conflicting functions.
- Static SOD will not tell you if between reports someone acquires access to conflicting functions, actually uses both, and then removes the access to the conflicting functions before the next report.
- Dynamic SOD controls, as implemented in AA, are based on real-time trigger-based auditing. They will tell you when a conflicting User-Responsibility assignment is made, or when a Responsibility or Menu is changed such that conflicting functions can now be accessed via a single Responsibility.
- AA's dynamic SOD controls will not tell you if, while someone has access to conflicting functions, they impact data using the two functions.

However, with AA's configurable trigger-based table auditing, which is also dynamic, you can detect when a business transaction actually happens, regardless of source or user. That complements and reinforces SOD controls implemented within the SOD Violations Manager.

Q-3. Do I need two function conflict lists, one for static SOD and one for dynamic SOD?

A. No. There is only one conflict list, and it is shared by the static reports and the dynamic conflict detection.

Q-4. What are the user watch lists in the E-Business Suite Extensions for SOD?

A. The user watch lists let you take a closer look at what selected individuals do, while ignoring the rest. You can also reverse the logic, and ignore what a few people do, but audit what everyone else does. A user list can be used in two ways:

- Watch List. Monitor a small group of users, while leaving the larger user population un-monitored.
- Allow List. This reverses the logic of the Watch List. Allow a small group of users access to certain functions, while monitoring the larger user population.

Note that you first must define an audit configuration for a table, then assign a user watch list to it. You can assign a user watch list to multiple tables. You can also assign multiple user watch lists to a table.

In both cases you are refining the selection criteria for when AA will respond to an audit event. Thus your controls are more targeted and exception-based.

Q-5. Can I start with SOD VM, and upgrade later to more of the Application Auditor functionality or extensions?

A. Yes, you can upgrade. First you would need to add the core AA product. After that, you can add either or both of the two add-on modules, in any sequence.

Adding AA by itself, you will be able to audit any table, and you would configure each new table audit, which could take from 5 to 30 minutes each.

If you then add the E-Business Suite Extensions for SOD, you will be able to get the dynamic SOD control, using the SOD conflict list you already have, to catch conflicting assignments when they are made. You would also be able to create and use User watch lists and allow lists. If you do use watch lists, you will have to use AA to create table audit configurations.

Finally, if you add the SOX Pack, you will be able to get table auditing for a very complete set of the tables our customers and advisors have found are relevant to SOX and other internal controls for the E-Business Suite. This could obviate the need to create audits on tables where you want to have user watch lists or allow lists.

Q-6. What if I don't want the 1200 SOD function conflicts you provide, but I do want SOD VM or the E-Business Suite Extensions for SOD?

In both cases you use the Conflict Manager screen to set up conflict pairs, document the controls, and assign exemptions to users. Since you create the pairs using picklists and lookups in an online form, it is easy to create and manage your own rules.

An SOD and SOX analyst at one of our customers was given a conflict list by their PWC auditor. She expanded on that, and created a spreadsheet of conflict pairs. The DBA imported the spreadsheet into the AA SOD VM, and thus had a conflict list that her company and the public auditor agreed on.

Q-7. Do you provide SOD and access reporting?

A. Yes. There are web-based reports you view in a browser window, as well as reporting views if you want to use Discoverer or other reporting tools. The web-based reports provide standard export to Excel for further analysis.

Using the AA views, the SOD and SOX analyst mentioned above developed a few Crystal reports in a matter of minutes. The internal and external auditors, and the IT and functional managers are very satisfied with the reports. A few SOD violations are found and reported most weeks.

Q-8. What if I want some users to have access to a pair of functions, but for everyone else it would be an SOD conflict and should be reported?

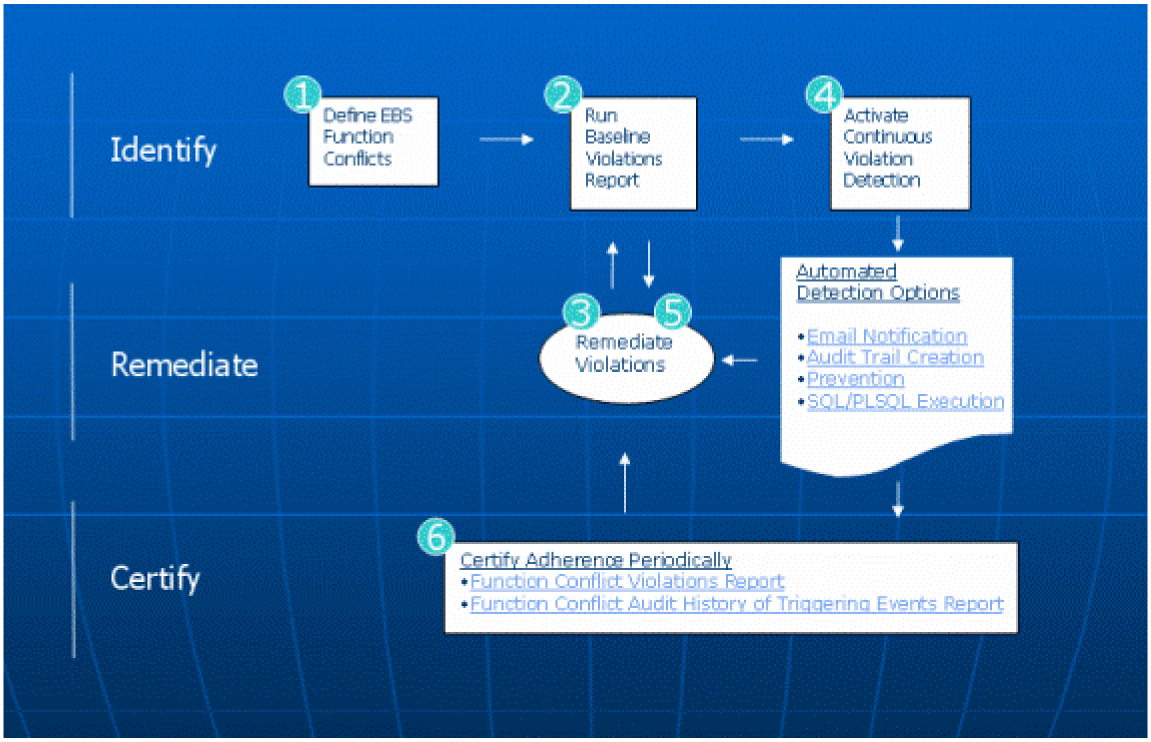
A. On the conflict manager screen, where you define conflict pairs, you can also grant exemptions to users, so their access to the conflict pair is not reported as an SOD violation.

Q-9. What if there's a sensitive function I want only a select few to have access to, and it's not necessarily in conflict with any other function?

A. You create an SOD conflict pair where the sensitive function is in conflict with itself. That way, your SOD reports will flag anyone who has access through any means. You also grant the select few an exemption to the conflict pair, so if they have access it is not reported as a conflict.

Q-10. What's the usual SOD compliance process with SOD VM or AA?

A. We found the compliance process for real time dynamic SOD control with AA can be divided into six steps. The process for static controls with SOD VM involves only the first three. See the following diagram and table.



		Step	
Application Auditor	**SOD Violations Mgr**	1. Define E-Business Suite Function Conflicts	▪ Select from 1,200 Pre-Defined Conflict Pairs ▪ Create Site-Specific Conflict Pairs
		2. Run Baseline Violations Report	▪ False-Positive-Free Logic
		3. Remediate Baseline Violations	▪ Process Owners Fix *Inter*-Responsibility Conflicts ▪ IT Staff Fix *Intra*-Responsibility Conflicts
		4. Activate Continuous Violation Detection	▪ Audit, Alert, Prevent
		5. Remediate Violations as Detected	▪ Process Owners Fix *Inter*-Responsibility Conflicts ▪ IT Staff Fix *Intra*-Responsibility Conflicts
		6. Certify Adherence Periodically	▪ No Reported Conflicts? ▪ User Responsibility Assignments Are Authorized and Current? ▪ Conflict Pairs Still Correct? ▪ All Triggered Violations Reviewed and Resolved? ▪ Application Auditor is Secure?

The first time through could require a large number of violations to be remediated. Most people recommend starting with Responsibilities and finding the Intra-Responsibility conflicts. When you're done remediating those, then it will be easier to re-run the baseline reports and work on the User-level Inter-Responsibility conflicts.

Q-11. Tell me more about Application Auditor.

A. You can select Oracle database tables to audit, configure the selection criteria and what before & after data from the audited table to capture, including data from related tables, and you can report all your audit configurations. The audit mechanism can also send email notifications and perform custom actions. You can also create an audit configuration to prevent a database transaction and record the attempt in the audit history table.

AA's audit mechanisms and reporting are more suited to business and finance auditors than many audit capabilities that are more technical in nature, that are used typically to instrument an application so you can debug it, or track workload. The standard database audit trail mechanism's main purposes are for fault recovery and supporting parallel instances.

AA's audit mechanism and business auditor workbench-like user interface are the foundation. By adding seeded configurations for E-Business Suite tables, we have been able to give EBS customers a head start in deploying SOX controls.

Similarly, the audit mechanism makes it easy to refer to our SOD conflict table in real time when User-level access changes are made in the EBS environment, and detect conflicts.

Finally, the audit mechanism can refer to our table of user watch lists to further refine how you implement SOD. You can use the user watch lists as either white lists or black lists, for flexibility.

Q-12. How about some details on the audit trails themselves?

A. First, you can configure the audits from multiple audited tables to be written to one or more audit trail tables. We believe it is easier to have a single audit trail table, for easier operations and to have a single source for reporting. However, this it is a customer decision at implementation time. Of course, you could change at any point; you're not locked in.

The audit trail table stores all change details from all of the related audited tables for efficient and flexible reporting:

- Before and After values of column.
- Table and Column name.
- Trigger Action (Insert, Update or Delete).
- Primary Key of Table.
- When and Who changed the column value.
- Session Details like IP Address, OS User, Session ID and Commit ID.
- Other column values within the same table at time of change, for context.
- Selected data values from other tables captured at the exact time of the transaction, again for context. An example is where you audit an order, and save the Customer ID from the audited table, but look up and also store the Customer Name from the Customer Master table.

Q-13. Can I populate an audit trail destination table other than the Audit Table provided?

A. Yes, any table in the current database instance.

Q-14. Can I use Application Auditor to track changes to EBS configurations and setups, and to master data like Customer or Product?

A. Yes. The SOX Pack of 90 seeded audit configurations includes these types of tables. The audit trails will track the before and after values of relevant columns, reference data, and also user and session information.

Q-15. Does Application Auditor support E-Business Suite R12?

A. Yes. Application Auditor can be used for these E-Business Suite releases: 10.7, 11.0, 11i, and R12 (all current versions) running on an Oracle database version 9i or greater.

Q-16. I'm going to upgrade from 11i to R12 soon. Can I deploy Application Auditor before the upgrade, and if I do, are there any special considerations?

A. There are no special considerations with deploying AA on the database for your 11i or R12 environment, or for when you upgrade from 11i to R12. There may be situations where you need to recompile or reconfigure the audit configurations or transport them from one EBS database instance to another, but these activities are provided in AA's user interface.

Q-17. Will I still be able to apply E-Business Suite patches and patch families, and add new modules?

A. Application Auditor has no impact on normal E-Business Suite operations, patches, or upgrades.

For your convenience and peace of mind, you may temporarily disable AA's audits at the click of a mouse and re-enable them after any non-standard DBA activity. However, AA has been known to identify undesirable activity performed by patch scripts. You may find AA, effective in preventing or highlighting patch issues.

Q-18. What happens if something does go wrong and I need to call Oracle Support?

A. If you think that the problem is related to Application Auditor or its extensions, please contact us. We will help you isolate and define the problem. When you contact Oracle, they may require you to recreate the problem and you may need to disable or remove the Application Auditor database triggers to help isolate the issue. This is the normal problem solving process with any ISV software component or CEMLI (customization, extension, modification, localization, integration). However, your audit configurations will not be lost and you will be able to easily re-create your audit triggers with the click of a mouse.

Q-19. Has Oracle certified your Application Auditor software to operate properly with the E-Business Suite?

A. No, and our customers have not required such certification. AA was developed using standards and guidelines Oracle recommends for extending the E-Business Suite. It also uses standard Oracle technology.

Q-20. How will I know if Application Auditor works in my E-Business Suite environment?

A. Our customers go through the usual change management testing processes, usually an abbreviated version. It is possible to test all the AA functionality in a few days, and we are happy to review your testing plan.

If in the production environment your other controls are working, and no transactions take place that would be subject to audit, then AA doesn't have much work to do or report. One customer occasionally injects transactions that trigger audits in production to see that AA is still working.

Q-21. It sounds too easy, what else is involved?

A. We believe it should be easy. Installation, testing, and deployment are straightforward. We have a document about the typical deployment project to which you may refer.

There are parts of the implementation project that will depend on the customer:

- Selection of which tables to audit. Our SOX Pack of 90 seeded audits for EBS makes this task easy. You simply select which of the 90 make sense for your environment, and review other tables you may additionally want to audit. Figure less than one hour to develop, test, and deploy an audit configuration.
- Selecting which function pairs cause an SOD conflict. Our 1200 seeded conflicts simplify the task. It takes a minute or so to add a new conflict pair.
- Deciding who should be on any user watch lists, and whether a list should be a white list or black list.
- When you first report SOD conflicts, there may be a large number. There are different remediation actions depending on your interpretation of the conflict and whether it is an Intra- or Inter-Responsibility conflict.

Q-22. What training do you provide?

A. There hasn't been customer demand for formal training. They find the User and Installation Guides sufficient, when coupled with our collaborative installation and deployment work. If questions occur later, you can contact us via email or phone for a quick response. We can work remotely via a web session with the customer if needed.

If your requirements include a training course for a group, we will provide that as an extra service.

Q-23. Will you help me design and deploy my SOX and SOD controls?

A. We usually provide a small amount of fee-based consultative support in how to use the software when you first license the software. Note that we are not SOX or financial controls advisors, so you may want to contact people who specialize in those areas or we can refer you to a specialist with whom we have worked. When you decide *what* you want to accomplish in terms of controls, then we can easily guide you in *how* to accomplish that using AA.

Q-24. How long does it take to implement and deploy Application Auditor? How about SOD VM?

A. The technical installation, implementation, and deployment take only a few person days of effort. Customers usually take between 2 – 4 weeks elapsed time, simply because the few people involved usually keep performing other work during the project. It is really customer dependent.

It takes just a couple of hours to install SOD VM. It's ready then to run reports using the seeded conflict list.

Q-25. Who needs to be involved with installing and running Application Auditor?

A. These are the roles and levels required for a typical Application Auditor implementation and deployment. A single individual can fill multiple roles based on their skills and the extent of support from Absolute Technologies. The level and amount of work to install and run SOD Violations Manager is considerably less. This table comes from our Implementation Project Overview document.

Organization	Project Role	Required Knowledge and Skills
Customer (may include Customer's consultants)	Project Manager (PM)	Experience in Oracle Database-based software product implementations. Coordinate and monitor project from initiation through production and post-production monitoring. Serves as liaison between Customer and Absolute Technologies.
	Business Audit Lead (BAL)	Experience in the areas of public accounting, internal auditing or consulting. Advanced understanding of Oracle E-Business Suite, business processes, and related IT controls like SOD , and Application configurations Some understanding of Oracle Database and Oracle Discoverer (or other reporting software) is helpful.
	System Administrator (SA)	Experience in preparing hardware, disk space, and logons for enterprise software deployments.
	Database Administrator (DBA)	Experience in the E-Business Suite and deploying enterprise wide software.
	IT Business System Analyst (BSA)	Experience with the E-Business Suite User Responsibilities and Menus

Organization	Project Role	Required Knowledge and Skills
Absolute Technologies	Consultant	Detailed knowledge of Application Auditor installation and configuration. Scope includes technical software installation, determining with the Customer the best configuration of audited tables, SOD conflicts, alerting mechanism, user watch lists, and informal user training.

Q-26. Do you use database triggers to audit the tables?

A. Yes. Our solution dynamically generates PL/SQL code to create a trigger and procedure combination that will track changes to selected columns of any table you specify. AA's Admin module also uses system triggers to audit database connections and DDL transactions.

Q-27. Do I have to re-key the audit configurations when I am ready to transport them to Production?

A. No. All you need to do is use the Migrate/Copy feature to move an audit configuration from one instance to another, or from one revision to another. A valid database link must be maintained for this purpose. Alternatively, you may use AA's Export/Import feature, which enables you to download/upload a copy of your audit configurations to/from a flat file. Once you have copied the configuration to a remote instance, you must compile it to active the triggers in order for it to begin creating the audit trail.

Q-28. Can I disable or turn off an active audit?

A. Yes. Via the online forms, you can toggle the status of the audit trigger from enabled and disabled.

Q-29. What if I get an error?

A. AA delivers robust error messaging and error handling via online forms. You may contact support for a quick evaluation and explanation.

Q-30. Do you provide a purge mechanism for the audit table?

A. Not in this release, but it is a simple matter that we have provided on a services basis. It will be added to a future release based on customer interest.

Q-31. Are there any restrictions to what you can audit?

A: The Oracle database does not support directly auditing tables owned by SYS. But any other table in the database can be audited. For more information regarding Auditing the DBA, please download our whitepaper at http://www.absolute-tech.com/download/Auditing_the_DBA_Whitepaper.pdf .

Q-32. What versions of the Oracle database are supported?

A. Release 9i and up are supported by the audit engine. However, the user interface requires Forms and Reports 6i or greater.

Q-33. Is AA integrated for use with Oracle E-Business Suite?

A. Yes and No. It is designed to work with any Oracle Database, not the E-Business Suite in particular. However, it may be installed into the same database instance as the E-Business Suite. AA may be purchased with extensions and auditor reviewed seeded content designed for E-Business Suite which support SOX and SOD audit functions.

Q-34. Our Oracle E-Business Suite environment is hosted by an outside service. Can I still use AA or SOD VM?

A. There are no technical reasons why you could not add either SOD VM or AA to your hosted environment. It depends on the arrangements you have with your service provider. We will assist you in discussions or deployment if you want us to work with them.

One customer is running SOD VM and E-Business Suite hosted by a major service provider. Oracle On Demand has approved SOD VM for use in their hosted environment.

Q-35. Why not use Oracle Application's audit trail feature?

A. The System Administrator audit trail feature is part of the E-Business Suite, and there are no extra licensing fees. If you have used this feature, you are aware that it is somewhat burdensome and limited in functionality. It creates a table and view combination for each table you audit, which makes it difficult to create a single report that provides all audit transactions. The audit record does not contain before and after values, additional reference table data or session details, and it does not provide an easy way to take inventory on all your audits. It does not provide for DDL or database connection auditing.

Application Auditor captures all audits in a single table regardless of how many tables you audit. And, it provides comprehensive reporting on all audits defined. Additionally, AA can collect information about a transaction that is not available with the Oracle Application audit trail feature. For example, it can capture before and after values, and session details such as the TERMINAL of the user making a change to the record. It can also run a user defined simple select statement at the time the column value is changed and store the result in the Audit table. AA's included Admin module provides DDL and database connection auditing.

Q-36. Why not use Oracle Governance, Risk, and Compliance Controls Suite?

A. Oracle's GRC Controls Suite is licensed separately from the E-Business Suite. The four components are:

- Oracle Applications Access Controls Governor
- Oracle Configuration Controls Governor
- Oracle Transaction Controls Governor
- Oracle preventive Controls Governor

Application Auditor provides the automation capabilities to support three of the above functions in your E-Business Suite environment: User access controls; setup and configuration controls; business transaction controls. AA also gives you the ability to prevent any kind of user access, configuration, master data or business transaction.

AA provides additional capabilities:

- It can be used to audit what DBAs and System Administrators do with the EBS database (DDL auditing).
- You can use the table auditing features on *any* Oracle Database, not just E-Business Suite.
- AA automates audit configuration migration and revision control, so you don't have to re-key your business rules and you'll always be able to fall back or review historical configurations.

We look forward to discussing your controls requirements and how AA can help.

Q-37. How can I learn more or get the software?

A. Please contact us at sales@absolute-tech.com or call 1-888-270-3012, or visit our website at www.absolute-tech.com.

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.

