Oracle® E-Business Suite

WHITE PAPER

Six Steps to Cut Compliance Costs

DECEMBER 2016

ORACLE Gold Partner

Q Software

Efficient, Sustainable Controls to Protect Your Business

www.qsoftware.com

For Oracle® E-Business Suite:

Six Steps to Cut Compliance Costs

CONTENTS:

US Headquarters:
4600 S Syracuse Street, 9th Floor,
Denver, CO 80237-2719
Tel: 303-256-6630

UK & EMEA Headquarters:
Connect House, Kingston Road,
Leatherhead, KT22 7LT United Kingdom
Tel: +44 (0) 1372 700852

sales@qsoftware.com

TRADEMARKS:
Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

ORACLE Gold Partner

Q Software

EXECUTIVE SUMMARY

Whether the driving need is to comply with statutory regulations or to reduce the risk of fraud, most organizations have evolved some kind of Internal Controls System to restrict system access to authorized users and to help them provide satisfactory evidence to their auditors.

Because Oracle E-Business Suite has limited inherent functionality to assist in this area, users have to seek other means of addressing their compliance needs. Most solutions are "off-the-box" and involve reporting on extracted data, which means that compliance reports reflect the status at a point in time, but cannot keep up with changes that are taking place on the live system. Some of the available solutions are costly and complex, involving lengthy implementation projects and significant investment in skills, software and hardware.

Consequently many companies have developed their own Internal Control Systems to address specific areas as needs arise. Typically the initial stage is to implement a method of reporting on Segregation of Duties (SoD), involving complicated spreadsheets and time-consuming manual checks to identify SoD conflicts.

But this approach cannot proactively **prevent** new risks being introduced when responsibilities are added or changed. Furthermore, the complexity and effort involved in this type of SoD reporting often makes it impossible to repeat it frequently, so new violations can sometimes go undetected for months.

To ensure accountability, the standard Oracle E-Business Suite auditing tools are difficult to use and have limited capabilities, making it hard to differentiate between normal day-to-day activity and unusual changes or transactions that may warrant investigation.

Automated controls, embedded in the Oracle E-Business Suite environment, yield significant savings in compliance effort and costs.

This paper describes a proven methodology and affordable, easy-to-use tools that empower Oracle E-Business Suite users to rapidly implement effective, sustainable controls in 6 key areas:

- Regular reporting to detect SoD conflicts
- Pro-active prevention of assignments that would introduce new SoD violations
- Automated Assignment provisioning with proactive SoD checking
- Automated Periodic Access Reviews
- Monitoring Master Data changes and material transactions
- Monitoring Configuration changes (for example where Responsibilities or approval limits are changed).

It explains how implementing these automated controls can significantly reduce the workload and cost of achieving and demonstrating compliance.

CREATING A MANAGEABLE SEGREGATION OF DUTIES FRAMEWORK

To protect the business and streamline compliance processes, most organizations have two main objectives in mind:

1. To identify and eradicate (or accept and mitigate) **any risk that already exists** in the system, such as Users who have access to combinations of functions that would allow them to commit fraud.
2. To **prevent new risks** from being introduced inadvertently as Responsibilities, Users and Functions are added and changed over time; where circumstances make new risks unavoidable, they must be highlighted and monitored.

Off the box solutions cannot pro-actively prevent Segregation of Duties violations.

Most manual and off-the-box systems seek to address the former, but are unable to carry out any kind of risk assessment at the Assignment Provisioning stage. The amount of effort involved in compliance reporting often means that the cycle is only completed, say, twice a year; with such a lengthy gap between reporting cycles, it is highly likely that many new conflicts will have been introduced in the meantime – which further extends the amount of effort needed to complete the next round of reporting and remediation – and so on.

The key to breaking this cumbersome cycle and making compliance manageable is to implement a robust Segregation of Duties framework ***within*** the Oracle E-Business Suite environment. This makes it possible to introduce automated conflict checking that can uncover existing risks AND check the impact of any new or modified User/Responsibility assignments as they are applied, warning you of any conflicts ***before*** they are introduced into the system.

THE PROBLEMS OF IDENTIFYING EXISTING RISKS IN THE SYSTEM

As noted above, the complexity and workload involved in the process often prohibit frequent checks. The tedious nature of the task also makes it prone to error, running the risk that SoD conflicts maybe remain undetected for long enough to allow fraudulent activity to take place.

Many Internal Controls Systems are only able to report on data extracted from the live system, rather than on the system itself, so take no account of subsequent changes. This means that compliance reports are often out of date and inaccurate before they are completed.

Complexity and labour-intensive processes often inhibit the effectiveness of identifying and eliminating risk.

With manual systems it is very difficult to achieve a sufficiently granular level of SoD reporting. Most organizations will design each Responsibility to be "clean" i.e. free from SoD conflicts within the Responsibility; then Segregation of Duties is implemented by designating that conflicting Responsibilities should not be assigned to the same user. But as a Responsibility may grant access to hundreds of

Functions via many menus, it is extremely difficult to ensure that no conflicts exist ***within*** the Responsibility, particularly if changes need to be made over time.

Similarly, as changes to Responsibilities are applied it is almost impossible to manually check that no new SoD conflicts are being unwittingly introduced ***across*** Responsibilities. Checking for conflicts at the function/task level, with all the possible access combinations, would be virtually impossible without automation.

Even where manual systems successfully highlight risks, there are no tools to help you remediate problems efficiently.

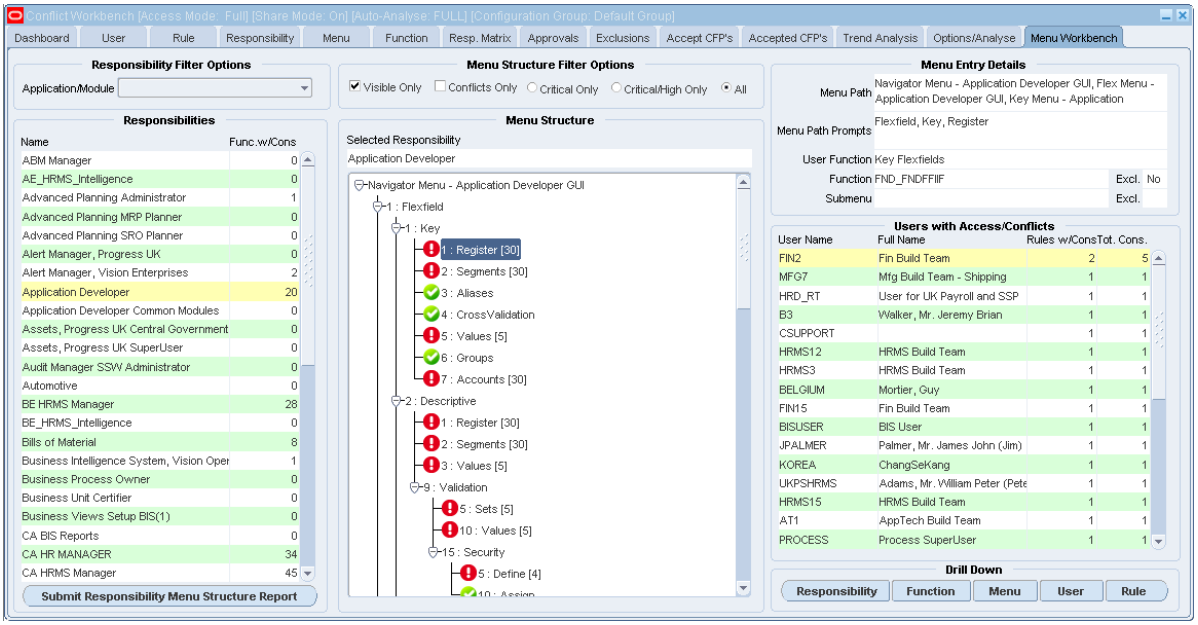
REGULAR REPORTING TO DETECT SEGREGATION OF DUTIES CONFLICTS.

CS*Comply, part of the CS*Applications GRC Suite for Oracle E-Business Suite, was specifically designed to overcome these issues.

It allows you to define a comprehensive set of SoD rules within the Oracle E-Business Suite environment, then the powerful conflict-scanning engine can analyze thousands of Responsibility / User / Function combinations in seconds to identify those which violate your SoD rules.

Pre-seeded rules speed up implementation of automated controls.

You can define your own rules, which can be as granular as you need them to be. Alternatively we are able to supply pre-seeded SoD rules sets, which include full documentation on the 20,000 Function based risks identified, and you can customize these as required. CS*Comply will also report on access rights to designated High Risk Single Functions, which can present a risk in their own right.



Results are presented to a Conflict Workbench for detailed analysis, where conflicts are rated according to their degree of risk, indicating priorities for remediation work. The workbench allows you to drill down to investigate issues so that you can address urgent issues quickly and efficiently. To avoid the danger of wasting time investigating spurious risks (for example where the access is via an enquiry screen that does not allow data to be input or amended), CS*Comply allows users to identify Common False Positives, which will then be excluded from SoD conflict enquiries and reports.

Segregation of Duties Reviews available on demand.

The speed and ease of the automated analysis process means that Segregation of Duties Reviews can be carried out on demand. As well as providing better protection against fraud, this also makes it much easier to answer auditors' questions quickly, speeding up the audit process.

PROACTIVE PREVENTION OF SOD VIOLATIONS

As the SoD framework is now built into the Oracle E-Business Suite environment, it becomes possible to check for potential SoD conflicts as Users and/or Responsibilities are being added or changed. The person making the changes will be notified of any conflicts arising from them. If there is a valid reason for the rule to be waived, for example to cater for staff absence, temporary access can be granted and will automatically expire on the specified end date.

AUTOMATED ASSIGNMENT PROVISIONING WITH PROACTIVE SOD CHECKING

CS*Provisum offers additional automation that exploits the built-in SoD framework of CS*Comply to streamline the process of Assignment Provisioning.

Assignment Provisioning is the process of granting a User access to one or more Responsibilities. For most organizations it is a time-consuming, repetitive process, where the security administrator (or other suitably privileged user) uses the standard Oracle E-Business Suite Users screen to assign Responsibilities. There is no means of checking whether the new Responsibility would introduce SoD conflicts.

Additionally, users have no automated ability to request access to Responsibilities, so many companies implement a manual procedure, such as filling in a paper form or submitting requests via email.

Such procedures tend to be inefficient and prone to error, as well as providing no reliable traceability as to who requested or approved what and why.

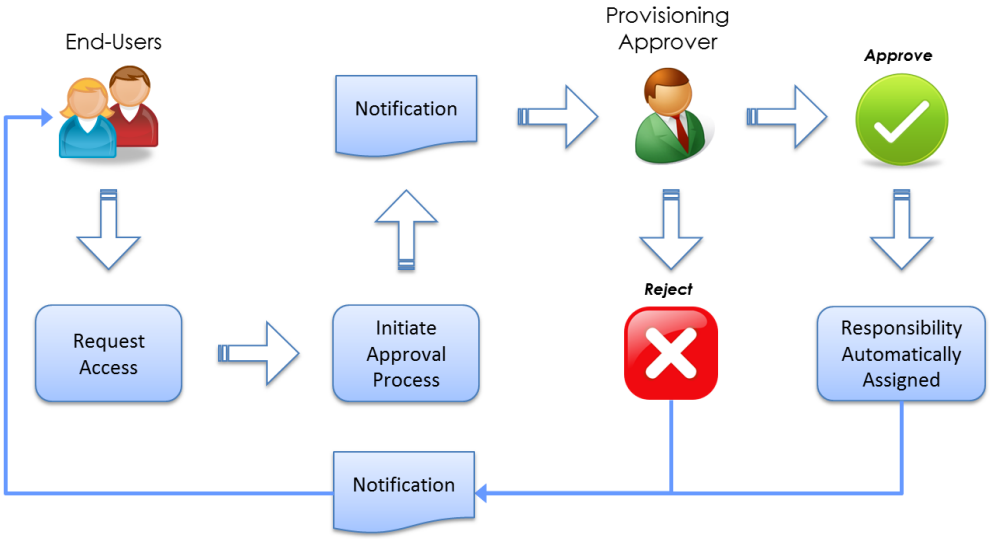
The Automated Assignment Provisioning function within CS*Provisum allows Users to submit access requests via the system.

Proactive SoD checks when new Users are created or Responsibilities are changed.

Once a request has been submitted, CS*Comply automatically runs the conflict scanning engine to determine the impact of approving a request from the SoD and high risk function access perspective.

The system then notifies an appropriate person, who can review the request then approve or deny it. Approved requests will automatically assign the Responsibilities as requested then notify the User.

Throughout the process, a detailed audit trail is generated to ensure full accountability.



AUTOMATED PERIOD ACCESS REVIEW

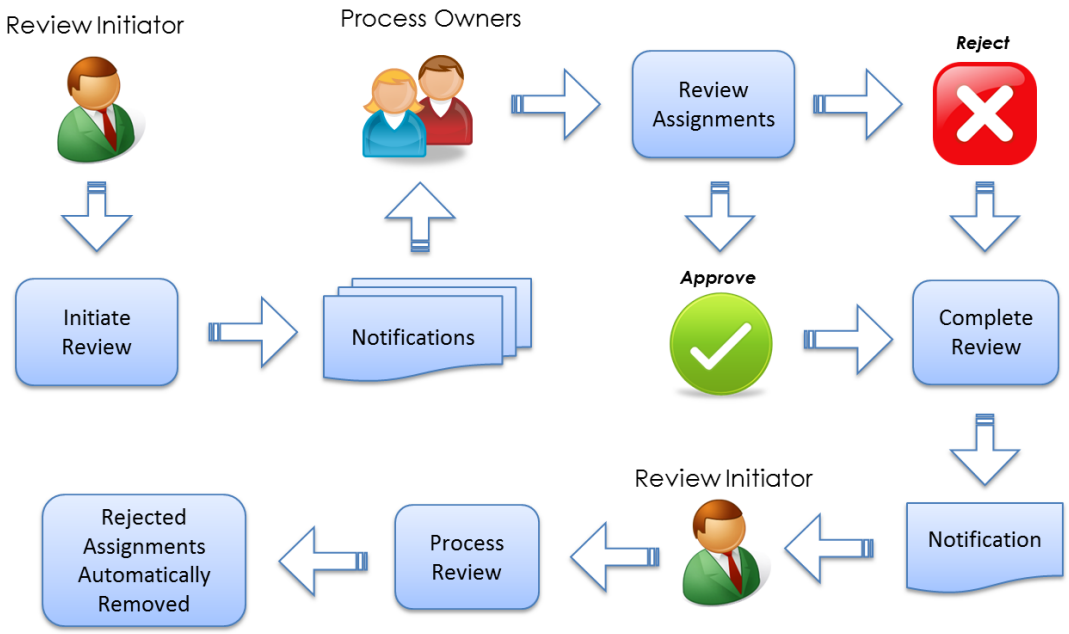
Businesses which are subject to Sarbanes-Oxley compliance are required to regularly review access to their systems. Most companies carry this out quarterly, and the process can drag out over such a long period that as one cycle ends, the next one is due to start.

Usually it is a manual process which creates a significant administrative workload.

During a typical Periodic Access Review, process owners (usually line managers or similar) review all Responsibility assignments for the areas that they have authority over. They approve or reject each assignment by updating a spreadsheet or annotating a report, then hand the results over to a security administrator, who actions the rejections by end-dating the relevant assignments. The initiator of the review wastes time chasing line managers and reminding them that the review needs to be completed; this can be a significant overhead for global organizations.

The information gathered during the review process is kept to help satisfy internal and external auditors that a proper assignment review is taking place.

CS*Provisum greatly reduces the workload by automating the process as illustrated below:



- Notifications are issued automatically.
- Process owners can check for SoD conflicts with CS*Comply before they approve assignments.
- Rejected assignments are automatically removed once the review is completed.

Equally importantly, the whole process is documented, with a complete audit trail of approvals and rejections, making it easy to provide the evidence required by auditors.

MONITORING MASTER DATA CHANGES AND SIGNIFICANT TRANSACTIONS

Most organizations need the ability to maintain a detailed audit trail to be able to find out who did what and when, as well as who approved it.

Oracle E-Business Suite does have standard audit functionality, but it is difficult to use and its capabilities are restricted:

- Although it is now possible to specify which columns in a table you wish to audit, the standard functionality does not allow you to specify conditional auditing (for example, you may wish to only log transactions where the value is greater than a specified amount.) This can generate huge amounts of data and make it very difficult to spot critical changes – you can't see the wood for the trees! Additionally, the standard auditing creates a shadow table of each table that is audited, further adding to the growth of data.

- Standard audit reports usually include lots of unintelligible codes and ID numbers rather than meaningful descriptions, making it difficult for business users to glean meaningful information. For example, instead of including Suppliers' Names, the reports identify accounts by the Supplier IDs, making them difficult to recognize. Similarly, Users need to know the correct IDs to be able to enquire or report on records relating to specific Suppliers.
- There is no means of documenting approved configuration changes on the system.
- Certain standard forms are not audited and there is no way of tracking activity carried out via SQL forms.
- There is no ability to notify someone when certain types of changes are made – so unauthorized changes or transactions may go undetected for a long time.
- Creating reports involves development time and resource which needs to be repeated for upgrades and when the business requires new reports.

External solutions are available to address these issues, but they are often complex, costly and very difficult to implement and use.

CS*Audit makes it much easier to maintain an effective audit trail and achieve full accountability.

Rules-driven auditing empowers you to focus on the events that need attention.

Its rule-driven auditing empowers you to specify exactly what should be audited and in what conditions, avoiding the need to trawl through massive data haystacks to check if there are any needles. If required, pre-seeded content is available to help you decide what to audit.

CS*Audit also enables you to include meaningful descriptions, such as Supplier Names, in the reports to make them easier to read, and approvals are documented as part of the audit trail. The powerful analysis and reporting tools make it easy to investigate issues and produce informative audit reports.

Automated notifications draw attention to unusual activity.

Critically, CS*Audit gives you the ability to **proactively** monitor data changes, however they are performed, as well as transactions. For example, changes to a supplier's bank account details, or transactions that fall outside of a specified value range can generate notifications to designated Users to draw their attention to unusual activity that may require investigation.

CS*Audit is installed out of the box with reports and analysis tools, avoiding the need for the development resources required by other auditing approaches.

MONITORING CONFIGURATION CHANGES

CS*Audit's proactive monitoring system can also be used to notify key personnel when critical configuration changes are made, such as granting someone the ability to approve payments, or making changes to approval limits.

As well as auditing Master Data and transactions, CS*Audit can keep a detailed audit trail of all critical configuration events, so that changes to Users, Responsibilities, Menus or Approval levels are all fully documented.

Where organizations need to monitor the differences between multiple Oracle E-Business Suite instances, such as development and production, CS*Impact provides a means of taking a "snapshot" of the systems and highlighting the variations on the screen, or detailing them in reports.

This gives technical teams a convenient way of assessing the impact of system changes before they affect users in the live environment – for example, if a menu is changed, it is possible that it will result in users having access to too many functions, or that someone will be prevented from accessing something that they need.

The snapshot function can also speed up problem diagnosis, by helping support staff to quickly identify changes that may have caused an issue.

It also provides a very useful tool for rapidly assessing the impact of Oracle E-Business Suite patches and updates, or for comparing changes between major versions during upgrade projects. For example, by identifying the differences in menus between R11i and R12, the changes can be accommodated to avoid significant disruption when upgrading the live environment.

PUT AN END TO THE DRAIN ON YOUR RESOURCES

If trying to fulfil your compliance obligations is costing you far too much, implementing automated controls could deliver results within weeks.

Embedded within the Oracle E-Business Suite environment, CS*Applications are easy to implement and use and require no additional hardware.

To discuss your requirements or request a demonstration, email sales@qsoftware.com or visit www.qsoftware.com

Q Software

An Independent Software Vendor and Oracle Gold Partner, Q Software delivers security and compliance solutions and services for users of JD Edwards EnterpriseOne, JD Edwards World, and Oracle E-Business Suite. Our products help customers to protect their businesses from fraud whilst significantly reducing the cost, effort and complexity of managing risk and demonstrating regulatory compliance.

ORACLE Gold Partner

Q Software