



ERP Seminars Risk-Based Automated User Access Controls Analysis

ERP Seminars is proud to offer its industry-leading risk assessment services in a *pre-packaged solutions* offering. We have teamed up with leading software providers to offer you an automated risk assessment using your data to give you a **real** assessment of risks in your environment.

NOT JUST SEGREGATION OF DUTIES! Our *risk-based user access controls analysis* goes beyond the traditional segregation of duties analysis to look at a variety of risks related to user access controls. We are the only firm using a truly risk-based approach to analyze user access controls and our thought leadership in the industry is unparalleled.

Integrated audit!!! Our analysis uses the only 'conflict matrix' that combines risks outside the system (such as access to cash, access to check stock, and the supplier approval and validation process) with the access control risks in your Oracle eBusiness Suite environment. Our assessment integrates the risk assessment process that external auditors use to analyze process control risks with the automated interrogation of access controls risks that an IT auditor would use – a truly "Integrated Audit."

Our conflict matrix was developed by analyst and industry thought leader Jeffrey T. Hare, CPA CISA CIA. Jeffrey's unique background and credentials has provided 'the perfect storm' to combine process and IT access risks into a single assessment process. This conflict matrix combined with automation software from various vendors will help you identify the greatest access controls risks in your Oracle eBusiness Suite environment.

To understand how to perform a proper risk assessment process, we suggest you request the white paper called "Risk-based Assessment of User Access Controls and Segregation of Duties for companies running Oracle Applications" from the Oracle Users Best Practices Board website (www.oubpb.com).

Why is our risk assessment process superior to other firm's assessment processes?
It's all about the rules! Let's look at an example in detail to see how our rules are built as opposed to how others are approaching the building of rules.



Others' approach to assessing risk:

Process 1	Process 2	Disposition / Comments - ERP Seminars	Risk Noted by Others
AutoAllocation Workbench	Generate Recurring Journals	See risks related to Mass Allocation at FC122. Having access to Generate Recurring Journals also does not increase the risk with access to Mass Allocations.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Daily Rates	See FC122 and FC128 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Period Rates	See risks related to Mass Allocation at FC122. Having access to Period Rates also does not increase the risk with access to Mass Allocations.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Historical Rates	See risks related to Mass Allocation at FC122. Having access to Historical Rates also does not increase the risk with access to Mass Allocations.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Import Journals	See FC122 and FC129 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Translate Balances	See FC122 and FC130 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Year-End Carry Forward	See FC122 and FC145 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Open and Close Periods	See FC122 and FC131 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation in the wrong period leading to misstatement of accounts
AutoAllocation Workbench	Post Journals	See FC132	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Generate MassAllocations	See FC13	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Generate AutoAllocation: Schedule	See FC13	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Generate AutoAllocation: Schedule	See FC13	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Consolidation Workbench	See FC122 and FC123 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Transfer Consolidation Data	See FC122 and FC133 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Transfer Consolidation Data Set	See FC122 and FC133 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Generate Eliminations	See FC122 and FC134 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation leading to misstatement of accounts
AutoAllocation Workbench	Common Stock	See FC122 and FC135 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.	Run inappropriate autoallocation leading to misstatement of accounts

The spreadsheet above is an example of what we call “Other Conflicts Evaluated.” We are continually looking at how other advisory and audit firms are evaluating risk and to the extent that we are presented new ‘conflicts’ that we have not evaluated before, we are documenting their disposition. In the case of the lines in yellow above, we have cross-referenced these risks to our rule labeled FC13, which you can see below highlighted in blue, which addresses this risk.

In the case where we see no real risk with the conflicts such as the example mentioned above highlighted in grey (between AutoAllocation Workbench and Common Stock), we are providing our reasoning and ‘commenting out’ the conflict.

Example based on Mass Allocations

There are a couple of things to point out in the spreadsheet above regarding how others approach the risk assessment. First, note that the “Risk Noted by Others” for all these ‘conflicts’ is the same (highlighted in green). Their risk noted is “run inappropriate autoallocation leading to misstatement of accounts.” The risk identified is what we call a single function risk because the risk is related to just having access to a single function, that being the AutoAllocation Workbench. The approach that many audit and risk-advisory firms have developed is to combine a single high-risk function with a combination of other functions that have *little or no relevance* to that function.

Refer to the line highlighted in grey. This is a good example of a single function risk (AutoAllocation Workbench) being combined with a function that has no relevance. This line indicates that having access to the AutoAllocation Workbench is in conflict with access to the Common Stock form. In the column labeled “Disposition / Comments -



ERP Seminars” the disposition states “See FC122 and FC135 - both are risks as single functions. However, there is no increased risk with the combination of the two functions.” In this example, both the AutoAllocation Workbench (i.e. Mass Allocations) and Common Stock forms have some level of “single function” risk associated with them. However, the combination of these two functions doesn’t add to the single function risk. One other comment before looking at our approach...

There are cases in which two functions that have “single function” risk do add risk when combined. An example is highlighted in blue below. In the case of access to AutoAllocation Workbench and Run/Generate Mass Allocations, both functions have single function risk. However, when a single user has access to both, there is additional risk. In this example, we have addressed the combined risk in our rule FC013.

Our approach to assessing risk:

Process 1	Process 2	Label	Business Process	Non-Risk Based Rank	Same?	System Related	Inherent Risk - see overall comment I	Pot'l Risk Mitigation - see overall comment O
Example 1 - Our Approach - consider single function risks and possibility of combine risks								
Maintain Mass Allocations	Maintain Mass Allocations	FC122	Financial Close	High	Yes	Yes	Changing of mass allocation formulas that are inappropriate or not approved by management. This could lead to inappropriate allocation of account balances and misstatement of financial statements	Audit and monitoring of changes to mass allocations by someone other than the person doing the maintenance. Once the generate Mass Allocations process was run, if someone were to review the outcome of those journals before they were posted or during the financial close process, the error(s) might be caught. Top level financial statement controls. See overall comment P.
Run Mass Allocations	Run Mass Allocations	FC153	Financial Close	High	Yes	Yes	Inappropriate timing on running of mass allocations resulting in allocation journals that are not appropriate or are unauthorized. This could result in the misstatement of financial statements	Once the generate Mass Allocations process was run, if someone were to review the outcome of those journals before they were posted or during the financial close process, the error(s) might be caught. Top level financial statement controls. See overall comment P.
Maintain Mass Allocations	Run Mass Allocations	FC013	Financial Close	High	No	Yes	Would allow someone to define and run a mass allocation which could result in a manipulation of financial data	Audit and monitoring of changes to mass allocations by someone other than the person doing the maintenance. Once the generate Mass Allocations process was run, if someone were to review the outcome of those journals before they were posted or during the financial close process, the error(s) might be caught. Top level financial statement controls. See overall comment P.
Common Stock	Common Stock	FC135	Financial Close	Low	Yes	Yes	Improper entry of common stock and dividend information could result in inaccurate EPS calculations which could result in bad decisions by management or inaccurate release of financial information relying on such underlying numbers	Top level financial statement controls. See overall comment P.

In our approach, we recognize both single function risks and the possibility that a user having two forms may result in increased risk. In the example above, there is inherent risk in both access to the **Common Stock** form and the **Maintain Mass Allocations** process. We also attempt to rank risks based on common business practices and likelihood of use of the form via the Non-Risk Based Rank. In this case, the ranking of risk related to the Maintaining and Running of Mass Allocations is “High” because of the powerful influence these processes can have on the account balances and, therefore, financial statements. We have ranked the risk of access to the Common Stock as “Low” because this form is not commonly used or, if used, there is likely a process to confirm the number of outstanding shares during the top level financial statement controls which would include a step such as this on a closing checklist (i.e. someone ties back from the 10K or 10Q to the report from the Stock Register).

SOD and Users Access Control Risks in Your Company

We recognize that the only way to properly address the risk of access to a single function or a combination of functions is to understand the possible mitigating controls



for YOUR company. This is the process we outlined in the white paper mentioned above (Risk-based Assessment of User Access Controls and Segregation of Duties for companies running Oracle Applications). In approaching SOD risks, some companies prefer to assess risk to reduce the list of rules to just those that are appropriate for their company. We have developed services based on this approach. If you want to perform a risk-assessment process and reduce the scope of the rules being used against your applications, this is offered as an optional service before running the automated assessment.

However, many companies approach their projects from the **big bang** approach. First, they would like to understand what risks there are in their system, then begin to research and document mitigating controls.

Our approach in this flat fee *automated controls analysis* is to analyze all possible rules against your environment and, where users have access that matches the rules, help you identify the risks. We also identify some common mitigating controls to give you some suggested ways companies have mitigated the risk(s).

Getting back to our example of the Mass Allocation process and how our process differs from others, the risk we cite for the single function access of Maintain Mass Allocations is "Changing of mass allocation formulas that are inappropriate or not approved by management. This could lead to inappropriate allocation of account balances and misstatement of financial statements." Our argument is that a user with access to this form could make a change to an allocation formula causing an inappropriate Mass Allocation journal entry which could lead to a misstatement in the financial statements. If you were to do a proper risk assessment process, you would look at the potential mitigating controls that could catch the error if the allocation formulas were inappropriately (i.e. not approved by management) or inaccurately (i.e. made in error) made. Three possible mitigating controls are cited as follows:

- Audit and monitoring of changes to mass allocations by someone other than the person doing the maintenance.
- Once the generate Mass Allocations process was run, if someone were to review the outcome of those journals before they were posted or during the financial close process, the error(s) might be caught.
- Top level financial statement controls. See overall comment P.

You can see from our example, that we are also evaluating other related single function risks. Highlighted in green is the **Run Mass Allocations process**. This process is also a single risk function. If the user that runs this process is different from the person(s) changing the Mass Allocation formulas, the Run Mass Allocation process could be run at the wrong time (i.e. before the formulas were changed), causing the allocation journals to be different than what was intended.

Finally, we recognize additional risk in a single user having access to both the Maintain Mass Allocations and Run Mass Allocations processes. In the case of these three risks (two single function risks and the combination of the two functions), the mitigating controls may be the same. For example, if there was a process to review all allocation journals before they are posted to make sure the results are as expected (for example, the allocation of rent expense to various departments based on headcount doesn't have a journal line to post to a revenue account), then the mitigating control may be the same.



However, if you have the AutoPost function set to automatically post allocation journals or if the person posting the allocation journal entries is not reviewing them, then there should be a heavier emphasis on the person maintaining the allocation rules. Alternatively, if there was not reasonable monitoring over the changes to the Mass Allocation formulas, you would have to rely on top level financial statement controls such as budget to actual analysis, flux analysis, and other items on your financial close checklist.

Further differentiation in our risk assessment process

There are three other significant differentiating factors in how we approach the risk assessment process versus traditional approaches:

1. Our approach takes into account risks outside the system
2. Our approach takes into account access to sensitive data
3. The automated analysis can be performed using a variety of technologies

Taking into account risks outside the system

Traditional risk assessment processes fail to adequately combine risks outside the system with access control risks. Let's look at a couple of examples:

Process 1	Process 2	Label	Business Process	Non-Risk Based Rank	Same?	System Related	Inherent Risk - see overall comment I	Pot'l Risk Mitigation - see overall comment O
Example 2 - Our Approach - understand the full process and take into account risks in manual processes outside the system								
Approve New Suppliers	Enter PO's	PP008	Procure to Pay	Critical	No	No	Collusion with suppliers for kickbacks / bribes to issue PO's. Risk ordering excess or unneeded inventory. If an approver can also be an initiator of a new supplier, this could allow the entry of a fictitious supplier and subsequent entry of PO(s) against such supplier.	See overall comment H for entity level controls that may help mitigate some of the risk. Three way match to the receipt could help mitigate the risk, if receipt is verified, and entered by someone other than the person issuing the PO. Inventory controls to review for excess or inappropriate inventory
Enter PO's	Enter PO's	PPH6	Procure to Pay	High	Yes	Yes	Entry of a PO, especially a two-way match PO, could lead to fraud. A weak supplier approval process would make this risk High (see overall comment A) because it may allow for the establishment of a fictitious supplier. Even without the establishment of a fictitious supplier, the entry of a PO in conjunction with collusion with a valid supplier could lead to fraud. See also overall comment J related to ERS / automatic invoicing of goods received. Two-way match PO's would allow for matching of invoices to the PO without a receipt which would likely be paid when payments are run in AP	Creation and auditing of invoice batches being separate from data entry could help mitigate the risk. However, it would be difficult to catch changes to invoices once the initial audit of the batch was performed unless a separate process was put in place for this as well. Implementing an invoice approval limit for each employee could help mitigate the risk. Requiring all AP invoices to be approved by someone other than the requestor / requisitioner would help mitigate the risk if the review for appropriateness of the expenditure was done. Top level financial statement controls. See overall comment P - in particular budget to actual and flux analysis.
Enter PO's	Line Types	PP137	Procure to Pay	Critical	No	Yes	Line Types determine whether or not receipts are required for PO lines and Receipt Close %. Access to change line types would allow someone to change this configuration which is often relied upon as a key control and is critical to the prevention of fraud. Access to both functions would allow a user to change a line type configuration and issue a PO with a two way match, for example. This could override automated controls such as the requirement to have a three way match.	Audit of changes and review by someone independent of the process to determine whether change was approved and considered impact on documented controls and efforts to prevent fraud.

Above are three examples of risks. The first one highlighted in blue has a conflict between the approval of new suppliers and the entry of a PO. The approval of new suppliers typically happens outside the system (there is new workflow functionality just introduced in version 12, but few companies are on version 12). If you don't take into account the risk that a buyer may be able to approve a supplier to be set up without any approval or that the approval of suppliers gets 'rubber stamped' when a buyer (or certain buyers) requests that a new supplier gets created, then you are missing a significant



fraud risk. If a buyer can get a fictitious supplier created and then issue a two-way match PO (receipt not required), he/she could create a fictitious invoice referencing the PO # and mail it into the AP department who would likely match it to the PO and pay it.

Also, the risk assessment process takes into account that in Oracle, even if you have defined the matching options to require a three way match in the Purchasing Options form, it can be overridden when a PO is created.

Taking into account access to sensitive data

Our risk assessment process also takes into account access to sensitive data such as personally identifiable information (PII), bank accounts, and credit card information. Such analysis is important to protect such data from check fraud and identity theft. Awareness of who has access to sensitive data will help to comply with sensitive data laws such as various state notification laws and PCI.

The automated analysis can be performed using a variety of technologies

Our thought leadership has given us an opportunity to work with a variety of industry-leading software providers. Several of these software providers have allowed us to offer these risk-based analysis services using their technology. This allows you to choose the one that best suits your company's needs. It could also provide the opportunity for you to compare vendors head to head with a proof of concept using the same set of rules.

Scope

The risk-based automated user access controls analysis will provide you with the following information and services:

From software provider:

- A. Conflict Details by Responsibility – which details the rules that were violated for each Responsibility (intra- Responsibility conflicts – Responsibility, Rule 1, User)
- B. Conflict Details by User – which details the Responsibilities and Rules within each Responsibility that violate the define Rules (User, Rule Name, Responsibility)
- C. Conflict Details by Rule – which details the Responsibilities and Users that violate each Rule (Rule Name, User, Responsibility, Conflicting Responsibility – could be the same as Responsibility where conflict is intra-Responsibility)
- D. Presentation of results – software provider will provide an overview of the results in a webinar format to allow you to interrogate the data and understand the use of the software, to the extent requested. Providers may offer additional services at their discretion.

From ERP Seminars:

- A. Summary of Conflicts by Rule – which details the rules, risks, and common mitigating controls. It will also identify the number of users that have the conflict.
- B. Presentation of Conflicts by Rule report – we will provide an overview of the probably higher risk areas based on your data. This presentation will be done remotely and include up to 4 hours. Optionally, for an additional fee, the presentation can be done on-site (see optional services below).



Pricing

ERP Seminars is pleased to offer our risk-based automated user access controls analysis using a variety of providers. Providers that will analyze your user access controls include Absolute Technologies, Approva*, CaoSys, Fulcrum Technologies, and Greenlight Technologies.

*some restrictions apply, contact us for details

Pricing is as follows:

Users *	Pricing (USD)
0 – 250	\$ 5,000
251 – 500	\$ 7,500
501 – 1500	\$10,000
1500 – 2500	\$20,000
Over 2500	Contact us for pricing

Note: number of users is based on non-self service users (excludes users, for example, that only have access to iProcurement and Employee Self-Service)

Optional services:

On-site presentation of results: additional \$1,800/day, plus travel expenses (contact us for locations outside the United States for further pricing considerations).

We will come to your company and present the results of the analysis to your executives and staff and work with you to identify the highest risk areas and prioritization of remediation.

Rules tailored to your company based on a full risk assessment: 1 to 3 weeks

If you want the rules tailored to your company based on ERP Seminars ERAM risk assessment methodology and our extensive conflict library, this can be done before or after the automated user access controls analysis. We will work with your staff to identify mitigating controls and analyze to what extent such controls mitigate the risks. Then, based on the residual risk, we will help identify what changes to your controls, business processes, or security is necessary. Additionally, we'll help you identify other areas of risk and research you should consider.

Recurring user access controls analysis – contact us for details

If you are interested in having the same rules run on a regular basis for controls testing or in preparation for your audit, we can provide a quote for using the entire rule engine or just those customized to your environment.

For additional information about these services, please contact sales@erpseminars.com.



FAQs

The following FAQs should help address some of the common questions and answers about the process.

Under what circumstances would I want to run this type of analysis?

Traditionally auditors have viewed Segregation of Duties as critical to fraud prevention and to internal controls best practices. However, because of the complexity of the security model in Oracle Applications, management has had a difficult time scoping the issue. The service could be used to provide an initial assessment of risk based on the way your company's security has been implemented. While we believe that most companies should consider implementing one of software solutions to activity detect and prevent SOD and other user access control risks, we recognize that many companies have chosen not to invest in a solution. The service could also be used on an on-going basis to review risks or to support or until a solution is implemented. The service could also be used in a pre-implementation (during User Acceptance Testing) environment where security is still being developed.

How is this service different than other services offered by other risk-advisory firms or audit firms?

This service combines multiple offerings into a single service. The analysis provides both a risk-based assessment process as well as an automated review of your user access control risks. The review of your user access control risks includes traditional segregation of duties risks as well as access to sensitive functions and access to sensitive data. We will also highlight some risks of process outside the system that, when combined with access to your Oracle Applications could allow a user to compromise the business process or commit fraud.

How does the process work?

The software providers will work with your IT staff to extract the data necessary to run the assessment. The extracted data is loaded in an instance in the software provider's secure environment and analyzed using ERP Seminars industry-leading risk based rules. As outlined in the Scope section above, both detailed and summary reports will be provided to you.

What involvement will I need from my IT department?

The scripts provided by the software providers vary. The time it takes to run in your environment depends on the number of users but generally take less than two hours in an average environment (less than 2,500 users).

Can I have the rules tailored to my company's controls environment?

A risk assessment can be performed prior to (or after) the running of the conflicts to reduce the rules to just those that are relevant to your company. Such services are not included in the fixed price scope. However, the scope of such services is generally one to four weeks.

What types of recommendations typically come as a result of the analysis?

In our white paper titled "Risk-based Assessment of User Access Controls and Segregation of Duties for companies running Oracle Applications," we have identified these types of results that come from a typically risk assessment process:

- An *SOD monitoring tool* (or one with a preventive workflow)



- A tool to develop a detailed audit trail
- Various monitoring reports or processes not provided by Oracle
- The need to personalize forms to support defined controls.
- Custom workflows to automate controls where Oracle's functionality is deficient
- Process and/or controls changes
- Documentation and testing of non-key controls
- Access control changes
- Additional projects and research that need to be done

Although the analysis provided by this flat fee, fixed scope service isn't a full risk-assessment, you can expect many of the same recommendations that we would make in a full risk assessment process, but the recommendations would be more generic in nature because we wouldn't have an understanding of your specific mitigating controls.