Protect Your Business and Reputation by Securing ERP Application Access

Employee access requirements create vulnerabilities, raise the potential for legal and financial liability

Adil Khan, CEO, SafePaaS

SafePaaS™

Oracle E-Business Suite

Business Application Access is becoming more of a concern due to the increased risk from providing ERP users capabilities or functionality that may be in conflict with the organizations' access policies. Auditors are focusing on the provisioning process, which is the initial point for granting access, in order to determine if sufficient controls are in place to identify and minimize potential risks.

This document outlines some of the major considerations in establishing and managing user application access.

Wide user access to diverse enterprise applications required to conduct business entails security risks

Security risks

- Standard user security administration tools (SoD, Segregation of Duties) within Oracle enterprise applications are insufficient to mitigate risks of fraud, financial misstatement and operational losses. Additional tools for access control security are required.
- Application access risks expand as businesses/organizations expand staff to execute required business processes. Poor access security controls giving to much access to an individual user can increase risks.
- Managers responsible for access controls often cannot obtain accurate function-mapped entitlement listings from enterprise applications, creating difficulty in building effective controls to enforce SoD policies.
- Access monitoring reports within the enterprise applications are not well designed to identify SoD violations.

User Access Provisioning tools such as Identity Management (IDM) systems operate at such a high level that they cannot see what is going on in an enterprise application at the user level.

They do not consolidate detailed user activity logs unless those logs pertain to the IDM administrators.

SafePaaS™

Mitigate risks with improved access controls

- Organizations require SoD access controls in ERP applications to mitigate the risk of fraud, waste and error. No single person should have the ability to complete two or more tasks within a business process that creates these risks.
- Many companies find it challenging to implement effective SoD controls in their ERP systems due to the complexity and variety of applications that automate key processes.
- To analyze the SoD risk that enables users in Oracle E-Business Suite to create a supplier and pay that supplier, you must identify all Oracle functions that constitute the entitlements granted through one or more responsibilities such as Payables Manager, Purchasing Manager, etc.
- Management needs to analyze the skill-set and capabilities of individuals involved based on the potential risk and impact to key business processes. Critical job duties can be categorized into four types of functions: authorization, custody, record keeping, and reconciliation. No one person should perform more than one type of function within the same business process.

You can apply the following options to segregate job duties:

- ***Sequential separation (two signatures principle)***
- ***Individual separation (four eyes principle)***
- ***Spatial separation (separate action in separate locations)***
- ***Factorial separation (several factors contribute to completion)***

SafePaaS™

Create access policies using the entitlements matrix

The entitlement matrix has been devised and used by many organizations as a method to determine access risks specific to an organizations ERP user security model. The following diagram is an example of an entitlement matrix.

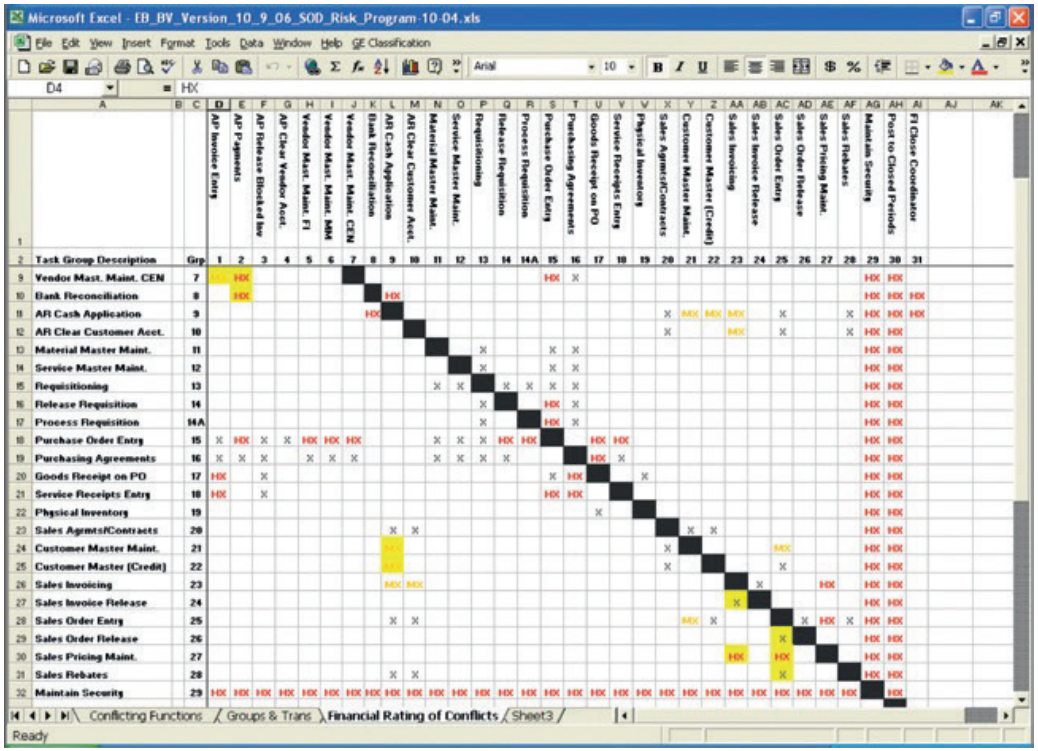


Figure 1: *Excel spreadsheet used to create Access Entitlement Matrix*

- *The Access Entitlement Matrix lists potential conflicts to determine what risk may be realized if a user has access or authorization to a combination of entitlements. For example, what is the likelihood that a user can create a fictitious supplier and make a payment to that supplier?*
- *The risk likelihood and impact varies based on industry, business model, and individual business unit. It is not uncommon for a large global company to have more than one matrix due to differences in business processes by location or business unit.*
- *Each business unit must perform a customized analysis of its conflicting access incidents in order to capture the real risk for that particular business model.*

SafePaaS™

Creating the risk assessment matrix

The following outlines the steps for creating an assessment matrix;

- The matrix provides a financial risk rating of access roles called "responsibilities" in Oracle E-Business Suite that are assigned to a user specifying with business functions available to them through the responsibility.
- Ideally, each responsibility should be designed to mitigate access control violation risks. A responsibility design consists of menus, functions and options a user can access to process business transactions and change data.
- The matrix comprises of the valid high-risk responsibilities that are aligned on both the X and Y axis, where the intersection between two responsibilities are marked to indicate the level of risk associated when an individual is given the requisite responsibilities.

Ensure access policy compliance

- It is important to test the security design to ensure that responsibilities granted to users do not grant access to conflicting entitlements causing SOD violations.
- Periodically test access control effectiveness by extracting the security configuration from security tables. This will provide the foundation to create an access violation program that tests security configuration for violations of access policies.

IT security can correct and access violations by removing entitlements from users and roles.

Auditors can use the "Access Violation" report to provide independent opinions regarding the effectiveness of access controls.

SafePaaS™

Evaluating User Access

Evaluating user access is a critical activity to minimize risk and comply with the organizations access policies. It is necessary to understand the components in order to make the necessary remediation recommendations to address the known incidents.

The diagram to the right is an example of user security model access structure.

Analyze access violations

- Violations of access polices must be analyzed to understand the basis for the violation which may indicate to change user access assignments and/or correct application security configurations.
- This analysis starts by examining the application function's level of access mapped in the rule sets in the relevant ERP security model. For example, Vendor-update rights may be executed through a series of Responsibilities, Menus and Functions, within the Payables and Purchasing applications.
- These should then be assigned to specific users should be verified, walked through and documented in order to accurately verify a particular conflict.

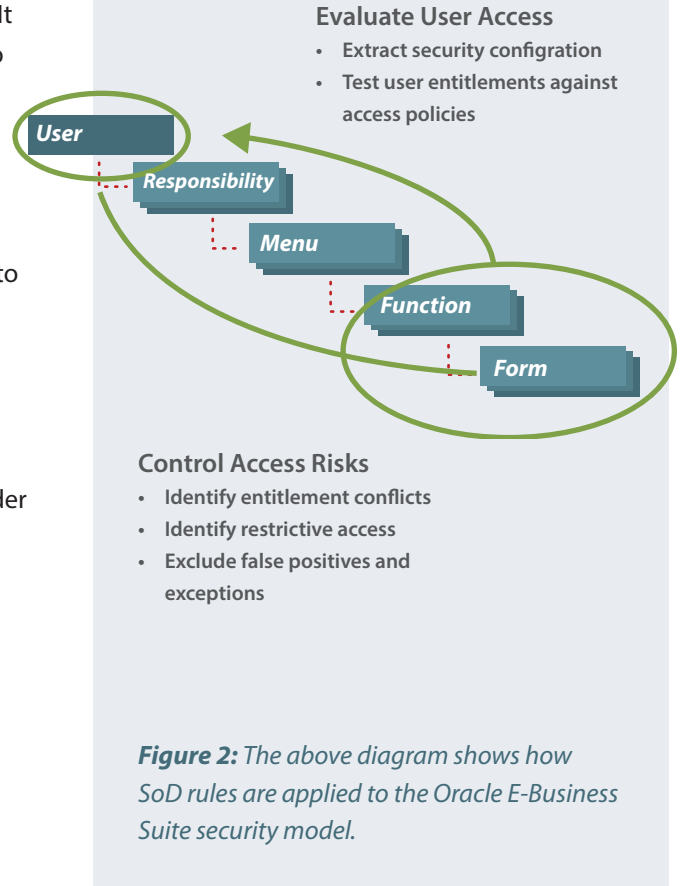


Figure 2: *The above diagram shows how SoD rules are applied to the Oracle E-Business Suite security model.*

SafePaaS™

User access management challenges

- In most modern applications there is more than one way to execute the same transaction;
- There may be 10 ways to pay a vendor in a payables application, but the company may use only five of them.
- The company is typically not aware of the other 10 ways and usually does not restrict access to or control these other methods to execute a vendor payment.
- Analyzing all the ways a user could potentially execute an application function is critical to accurate remediation and prevention of access risk.
- Users are provided multiple roles or responsibilities providing multiple access paths to the same transaction.
- Remediation through changing roles or responsibilities have an undeterminable effect to users where no violations are identified.

The access violation analysis requires that you discover all the potential methods for executing a transaction in order to understand the full potential for fraud, not just the limited view of the known methods.

SafePaaS™

Access management challenges increase risk

Businesses and other large organizations are challenged to ensure an effective and efficient access management process with a growing assortment of Cloud, on-premise and mobile applications. These challenges can result in management fatigue, materialized risk and operational losses in the following areas:

- User access requests, are manually processed through various fragmented channels and ERPs, are without effective audit trails, waste time and money.
- Lack of visibility into potential access policy violations during the provisioning process can compromise the security of enterprise applications and sensitive data such as financial statements, customer orders and supplier payments.
- Companies can lose reputation with headline making security breaches if vulnerabilities in unprotected systems are exploited from outside or inside.
- Provisioning individual users multiple roles or responsibilities causing unknown access risk during the provisioning process.

SafePaaS™

User access request management

In most organizations, application user provisioning is a manual process complicated by multiple applications, inconsistent user security models for each application, complex access policies, and lack of detailed understanding of each application. The following diagram demonstrates the potential complexity of the provisioning process.

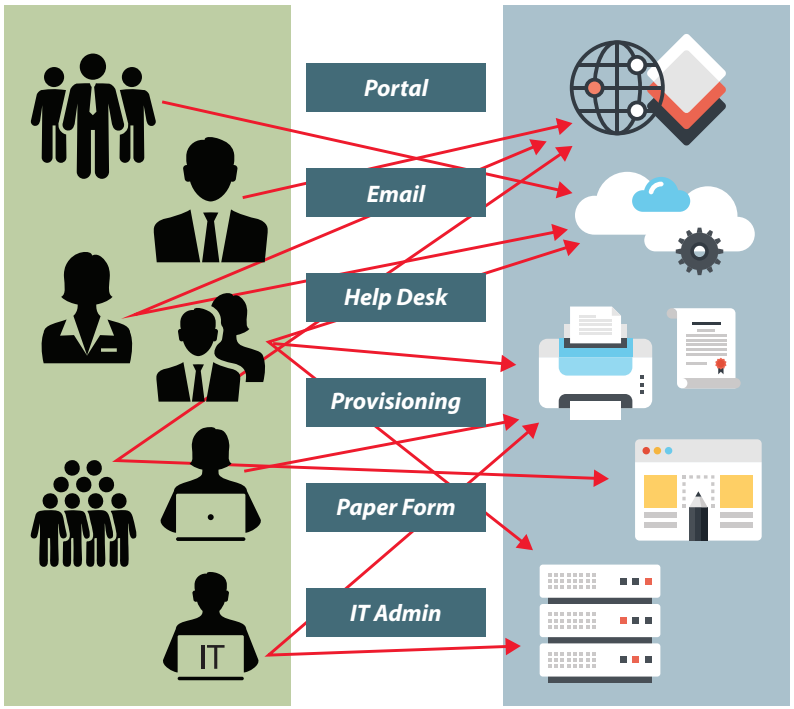


Figure 3: *Access risks created by multiple and conflicting authorities*

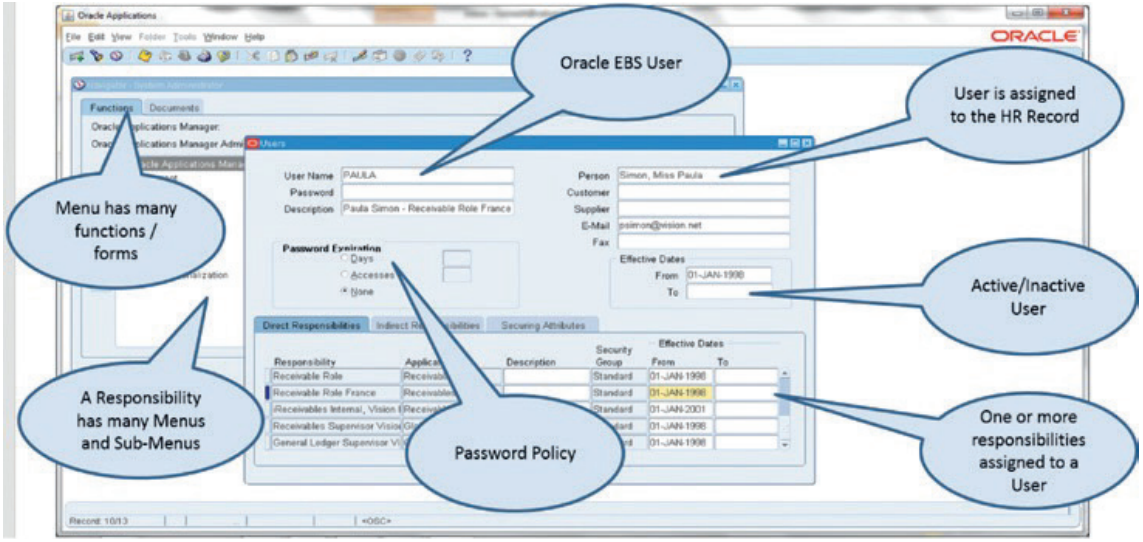
- *As shown to the left, large organizations process hundreds of users every day, adding, changing and deleting requests received through multiple sources—emails, paper forms, help desk tickets, etc.*
- *The user request process is inconsistent, ad-hoc and platform dependent. It is difficult to test access requests against company polices.*
- *Approval request is granted without testing the security risks against policies at the functional level. Auditors cannot rely on the access controls and require management to manually test application access.*
- *Lack of common access controls and centralized audit trails increases the threat of data breach and cost of audits. IT security and management are burdened with time-consuming remediation tasks.*

SafePaaS™

User access assignment

The following points identify a typical user access governance;

- User access assignment in ERP applications requires a security administrator to enter or update user details (user ID, password) and associated employee information.
- The standard application user assignment process is inefficient and inconsistent – it does not prevent security administrators from granting access to one or more roles that may violate an access policy.



External audit firms are increasing focus on application access management testing as regulations around the world require companies to comply with data privacy policies and ensure the effectiveness of internal control over financial statements.

Seven of the top 10 control deficiencies relate to user access control.

Figure 4: *The screenshot of the Oracle E-Business Suite User Security Form shows all the direct, as well as indirect, user security and functional assignment attributes granted without any preventive policy enforcement.*

SafePaaS™

Access Control Deficiencies

The following are common access control deficiencies;

- Ineffective access request management – limited audit trails, lack of visibility into potential access policy violations – leaves mission critical systems unprotected against data breach, fraud and financial misstatement risks.
- Deficient application access controls are a common source of internal abuse and a top focus for IT audits.
- 44% of IT audit deficiencies are related to user access management.

Figure 5: *The diagram shows the common access control deficiencies reported by auditors.*

SafePaaS™

Automated access controls management

There are methods to automate and streamline the application access controls management process. Doing so enables an organization to:

- Monitor access policies with user and responsibility violation reports.
- Manage access roles to remediate violations by excluding functions from responsibilities or roles, by simulating the impact and deploying corrected security models.
- Deploy a self-service user provisioning workflow that provides access risk information to approvers to ensure access policy violations are prevented before a user is assigned responsibilities or roles.
- Certify user access to assigned responsibilities by notifying manager of user access and capturing information to disable access that is no longer required.

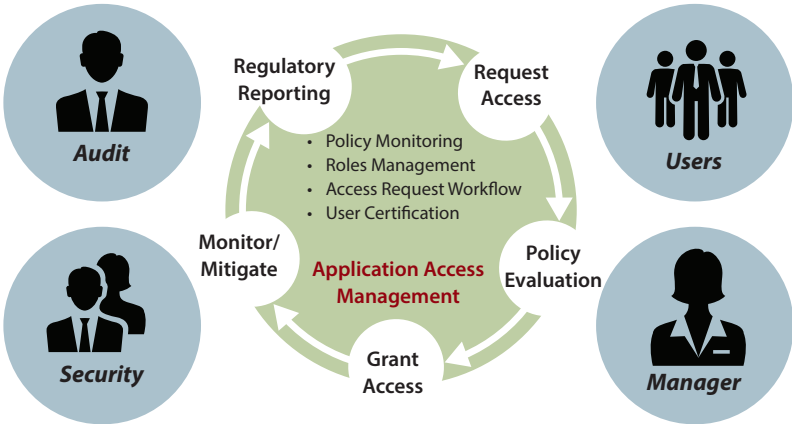


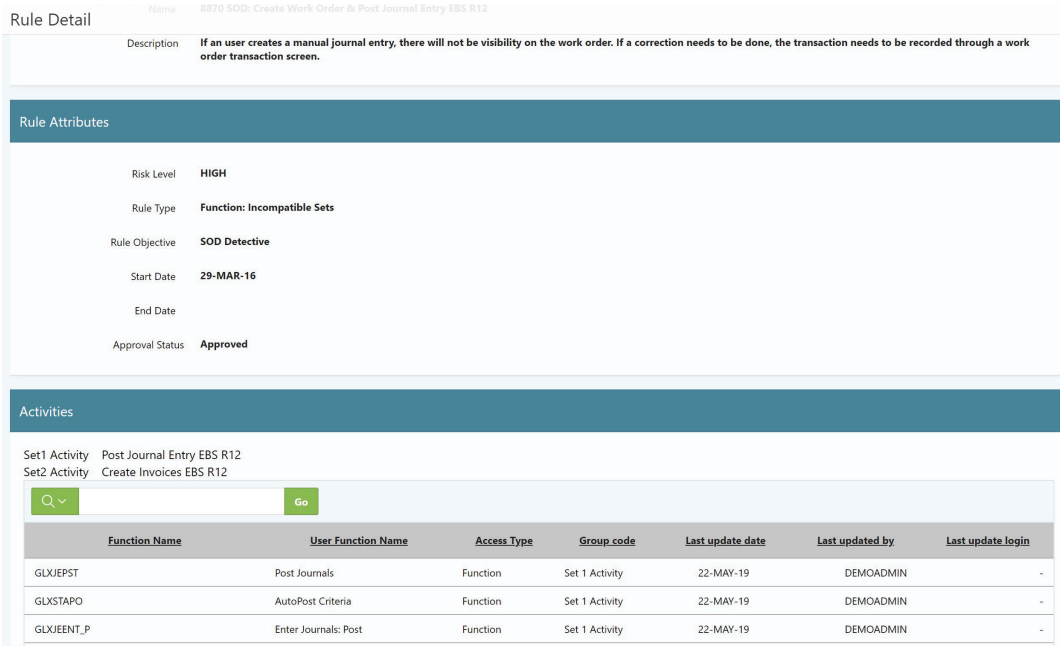
Figure 6: *The diagram shows the complete access controls management life-cycle.*

SafePaaS™

Monitor policy compliance

With the establishment of an access controls framework, you need to continually monitor the policy incidents with the following:

- Once you have established the entitlement matrix based on access risks identified by management, you can create access rules that identify conflicting business activities.
- In Oracle E-Business Suite activities are assigned to users through responsibilities which enable the user to access functions on forms and pages through menus.
- To monitor policy compliance in Oracle you must define function sets that enable business activities.



Rule Detail

Name 8870 SOD: Create Work Order & Post Journal Entry EBS R12

Description **If an user creates a manual journal entry, there will not be visibility on the work order. If a correction needs to be done, the transaction needs to be recorded through a work order transaction screen.**

Rule Attributes

Risk Level	**HIGH**
Rule Type	**Function: Incompatible Sets**
Rule Objective	**SOD Detective**
Start Date	**29-MAR-16**
End Date	
Approval Status	**Approved**

Activities

Set1 Activity Post Journal Entry EBS R12
Set2 Activity Create Invoices EBS R12

Go

Function Name	User Function Name	Access Type	Group code	Last update date	Last updated by	Last update login
GLXJEPST	Post Journals	Function	Set 1 Activity	22-MAY-19	DEMOADMIN	-
GLXSTAPO	AutoPost Criteria	Function	Set 1 Activity	22-MAY-19	DEMOADMIN	-
GLXJEENT_P	Enter Journals: Post	Function	Set 1 Activity	22-MAY-19	DEMOADMIN	-

Figure 7: *The screenshot to the left shows a SoD rule to detect use access violations when a user can both "Create Supplier" and "Create a Payment for that Supplier"*

SafePaaS™

Assessing access risks in Oracle

Below is an example of how to assess a common access risk:

- There are five functions in Oracle to create suppliers and six functions to pay suppliers.
- The grouping of functions into business activities enables business managers and security administrators to assess the business risk as well as make remedial technical configuration changes.
- Once a rule is created you can run the access violations program to test the rule against a "snapshot" of the ERP security tables where user and responsibilities do not comply with policy. The results can be viewed in an access policy violations report.

AccessPaaS \ Policy Manager \ Define Scope \

Manage Rules

Environment: OracleEBS_R1229

Go | 1. Primary Report | Actions | Add Rule | Filter False - Positives | Import Rules | Export Rules

Name	Description	Risk Level	Rule Type	Rule Objective	Approval Status	Version	Start Date	End Date	Activity1	Activity2	Last Update Date	Last Updated By	Rule Owner
9999 - Incompatible Sets	9999 - Incompatible Sets	MEDIUM	Function: Incompatible Sets	SOD Detective	Approved	2	13-APR-21	-	Post Journal Entries - EBS R12	Enter Journal Entry EBS R12	14-APR-21	DEMOADMIN	Owner => RENDERS
Sensitive Access - Post GL Journals	Sensitive Access - Post GL Journals	MEDIUM	Restricted Access	Restricted Access	Revised	4	27-OCT-20	-	Post Journal Entry EBS R12	-	10-SEP-21	DEMOADMIN	Approver => ROBERT; Owner => ADIL, RENDERS
Open and Close GL Periods AND Post Journals	Open and Close GL Periods AND Post Journals	HIGH	Function: Incompatible Sets	SOD Detective	Approved	2	12-DEC-19	-	Post Journal Entry EBS R12	Open Close General Ledger periods - EBS R12	23-APR-20	DEMOADMIN	Approver => ROBERT; Owner => RENDERS
Post Journal and Bank Reconciliation - ConEd	Post Journal and Bank Reconciliation - ConEd	HIGH	Function: Incompatible Sets	SOD Detective	Revised	2	12-DEC-19	-	Bank Account Reconciliation EBS R12	Post Journal Entry EBS R12	14-FEB-20	RENDERS	Approver => ROBERT; Owner => RENDERS, ROBERT; Reviewer => DEMOADMIN
9000 GL Sensative Access	General Ledger Sensitive Access	HIGH	Restricted Access	Restricted Access	Approved	2	18-NOV-19	-	Post Journal Entry EBS R12	-	19-NOV-19	RENDERS	Owner => RENDERS
Enter Customer Credit Limit & Release Hold on Sales Order	Enter Customer Credit Limit & Release Hold on Sales Order	HIGH	Function: Incompatible Sets	SOD Detective	In Approval Progress	1	05-JAN-18	-	Enter Customer Credit Limit - MVL	Release Holds on Sales Order - MVL	05-JAN-18	RENDERS	Approver => DEMOADMIN; Owner => CAROLYN; Reviewer => RENDERS

Figure 8: *The screen shot to the left shows that a user has the potential access risk of creating a supplier and paying that supplier. The report shows the responsibilities, menus and functions in each row that allow the user to access conflicting business activities.*

SafePaaS™

Steps to remediate access control defects

Remediation is a key task to address access control incidents where policies have determined the existence of a violation. Remediation involves multiple participants from the business, audit and Information technology to determine the appropriate correct action. Below are the following considerations for remediation:

- Access risk remediation requires two major types of corrective actions.
  1) When a user has access to conflicting entitlements that pose "inherent risk" the security configuration in the application requires updating.
  2) Reassigning user roles where the violation is caused by the user having access to two or more conflicting roles.
- User role security configuration is the root cause for the majority of access policy violations, but updating roles in an ERP system with hundreds or thousands of active users can negatively affect business performance.
- Companies and auditors get bogged down during remediation because of the difficulty in changing security design allowing business users to perform their tasks.
- We recommend automating the role redesign process by analyzing source roles with violations and creating "target" roles that can be reconfigured and tested for access policy compliance before deploying the compliant roles into the production system.

SafePaaS™

Correcting roles with access policy violations

Correcting roles is a common occurrence in the remediation process. The ideal is to make any corrective actions in the ERP application as there may be a cascading affect impacting multiple users with the change to a single role.

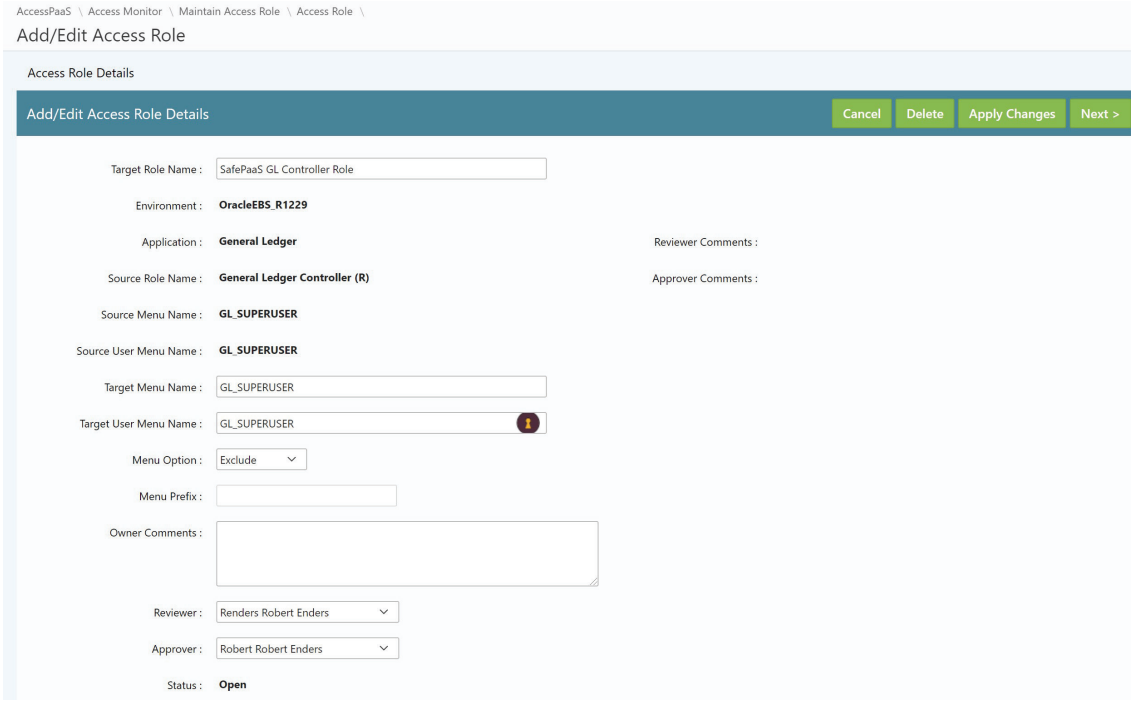


Figure 9: *The image to the left shows a new target role "FWY Payable Manager" derived from the source role "payables Progress UK Super User" in Oracle E-Business Suite*

- *This role has a number of SoD access policy violations including "Create Supplier" and Create Payments."*
- *Correct the violation: Use exclusion tool in Oracle User Security Form to exclude all functions associated with the "Create Supplier" entitlement.*
- *The following figure shows a tool that allows for changing roles or responsibilities as a key part of the remediation process without requiring detailed technical knowledge of the ERP.*

SafePaaS™

Correcting roles with access policy violations cont.

SOD Violation Summary SOD Violation Details

SOD Violations

Go Actions

Rule Name	Rule Description
6870 SOD: Enter Journal Entry & Post Journal Entry EBS R12	Financials
7180 SOD: Mass Allocate Journal Entries & Enter Journal Entry EBS R12	Financials
Open and Close GL Periods AND Post Journals	Open and Close GL Periods AND Post Journals
7700 SOD: Post Journal Entry & Set Up GL EBS R12	Financials
6910 SOD: Enter Journal Entry & Set Up General Ledger EBS R12	Financials

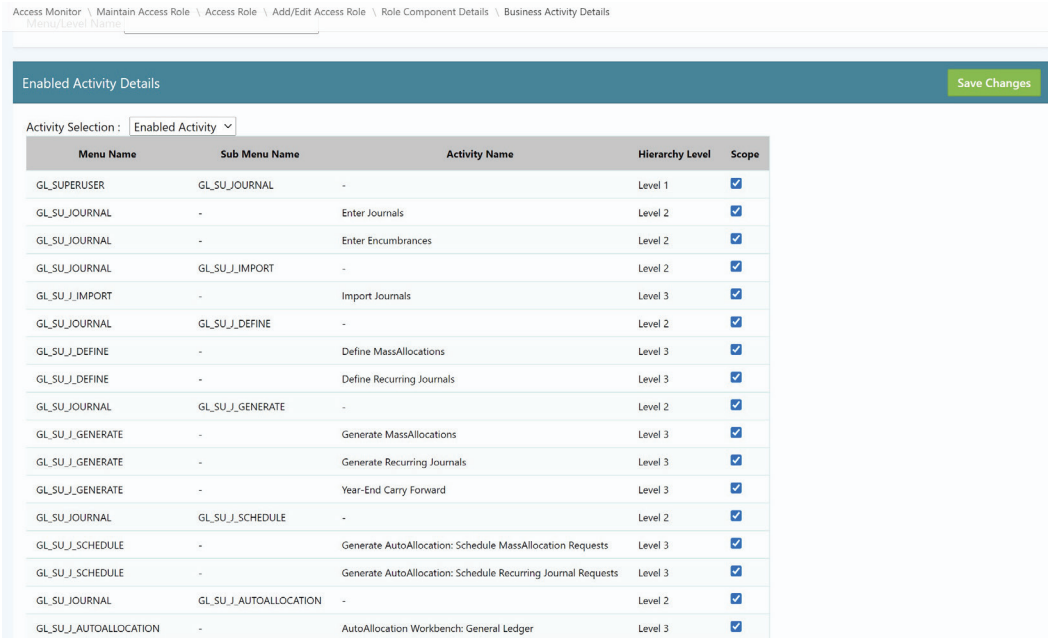
Figure 10: *Exclude "Create Supplier" functions by checking them off in form.*

SafePaaS™

Provision users with policy compliance

The user provisioning process provides an opportunity to prevent access violations through an automated work-flow for review and approval process. These include:

- Once user access violations the ERP system have been detected and remediated, it is important to prevent violations from recurring as new user requests are processed and the security model is updated to meet new business requirements.
- New users' role assignments must be tested for access policy impact when changes are made in order to prevent repeating remediation process during next audit cycle.



Menu Name	Sub Menu Name	Activity Name	Hierarchy Level	Scope
GL_SUPERUSER	GL_SU_JOURNAL	-	Level 1	☑
GL_SU_JOURNAL	-	Enter Journals	Level 2	☑
GL_SU_JOURNAL	-	Enter Encumbrances	Level 2	☑
GL_SU_JOURNAL	GL_SU_J_IMPORT	-	Level 2	☑
GL_SU_J_IMPORT	-	Import Journals	Level 3	☑
GL_SU_JOURNAL	GL_SU_J_DEFINE	-	Level 2	☑
GL_SU_J_DEFINE	-	Define MassAllocations	Level 3	☑
GL_SU_J_DEFINE	-	Define Recurring Journals	Level 3	☑
GL_SU_JOURNAL	GL_SU_J_GENERATE	-	Level 2	☑
GL_SU_J_GENERATE	-	Generate MassAllocations	Level 3	☑
GL_SU_J_GENERATE	-	Generate Recurring Journals	Level 3	☑
GL_SU_J_GENERATE	-	Year-End Carry Forward	Level 3	☑
GL_SU_JOURNAL	GL_SU_J_SCHEDULE	-	Level 2	☑
GL_SU_J_SCHEDULE	-	Generate AutoAllocation: Schedule MassAllocation Requests	Level 3	☑
GL_SU_J_SCHEDULE	-	Generate AutoAllocation: Schedule Recurring Journal Requests	Level 3	☑
GL_SU_JOURNAL	GL_SU_J_AUTOALLOCATION	-	Level 2	☑
GL_SU_J_AUTOALLOCATION	-	AutoAllocation Workbench: General Ledger	Level 3	☑

SafePaaS™

User request workflow

Key to an automated user provisioning process is the review and approval workflow to the appropriate business process owners. A flexible workflow engine assists an organization with review and approvals that vary based on business process or level of access.

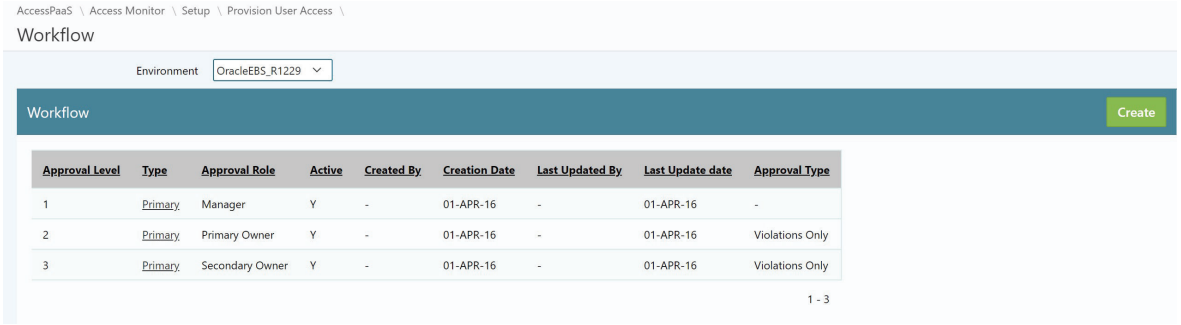


Figure 12: *Approval levels and roles for user access requests.*

- *The first step in setting up a user access request workflow is to determine the approval levels and roles. The workflow in Figure 12 has three levels of approval:*
- *The employee's manager is the first approver. Manager information is obtained from the HR tables as part of the ERP security "snapshot" that is processed at a frequency defined by management.*
- *Next, the request goes to a primary and a secondary approver. The primary approver can be a "functional" manager familiar with the functions in the requested Oracle Responsibility. A technical manager with understanding of the Oracle security model may be assigned as a secondary approver.*

SafePaaS™

User requests for new responsibilities

Once the workflow is configured and approvers are assigned a registered user can use the access request page to access new responsibilities as in the image below.

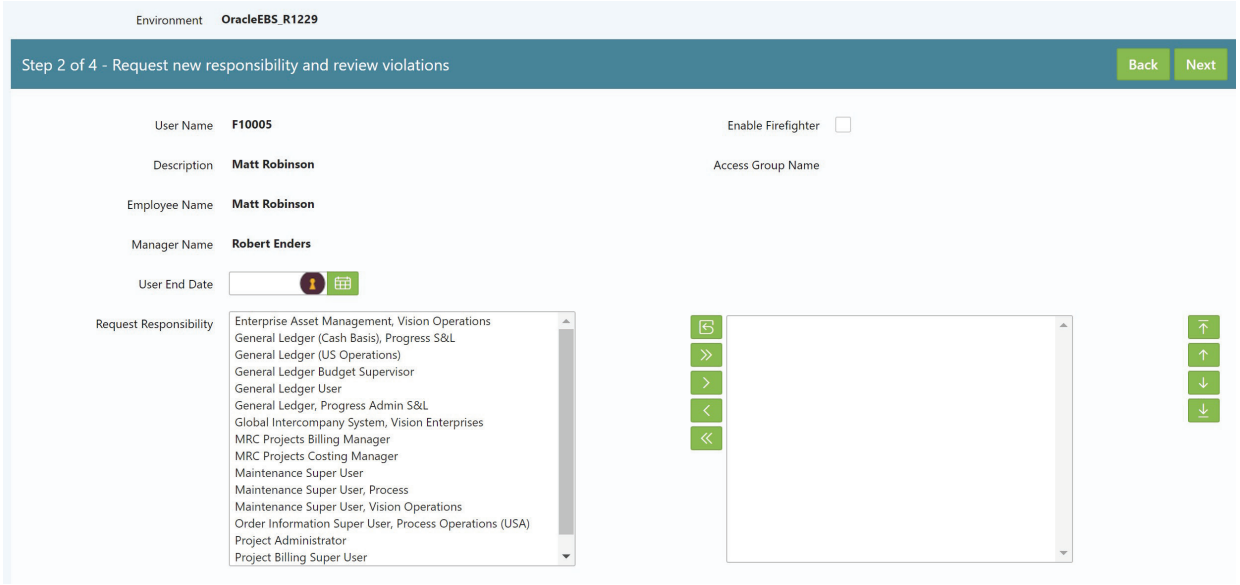


Figure 12: *The screen shot shows a user requesting Payables Vision Services R&D responsibility:*

- *The user access request is routed by the pre-configured workflow to each person assigned an approval role. The IS Security Administrator can monitor all access requests and change or cancel a request if required.*

SafePaaS™

User requests status and auditability

User provisioning automation allows for the ability to review status of a request, but also to audit all requests to determine who and when approved access for a particular user. This ensure more effective audit of compliance with the organizations access policies.

AccessPaaS \ Access Monitor \ Setup \ Provision User Access \

Request Status

Environment OracleEBS_R1229

Request Status

Go | 1. Primary Report | Actions

Ref#	Network Id	Name	Email	Approval Status	Requested Date	Requested By	Responsibility Key	Responsibility Name	Start Date	End Date	Requested	Approval Level	Type
38640	F10002	Kumar Nadar	bizdev@safepaas.com	Pending	03-JAN-2022 16:27	RENDERS	PRG_GL_SUPERUSER_CASHBASIS	General Ledger (Cash Basis), Progress S&L	03-JAN-22	-	Yes	1	Primary
38640	F10002	Kumar Nadar	bizdev@safepaas.com	Pending	03-JAN-2022 16:27	RENDERS	PRG_GL_SUPERUSER_CASHBASIS	General Ledger (Cash Basis), Progress S&L	03-JAN-22	-	Yes	2	Primary
38640	F10002	Kumar Nadar	bizdev@safepaas.com	Pending	03-JAN-2022 16:27	RENDERS	PRG_GL_SUPERUSER_CASHBASIS	General Ledger (Cash Basis), Progress S&L	03-JAN-22	-	Yes	3	Primary
38639	F10031	Dan Smith	bizdev@safepaas.com	Pending	03-JAN-2022 16:22	RENDERS	PRG_GENERAL_LEDGER_USER	General Ledger User, Progress S&L	03-JAN-22	-	Yes	1	Primary
38639	F10031	Dan Smith	bizdev@safepaas.com	Pending	03-JAN-2022 16:22	RENDERS	PRG_GENERAL_LEDGER_USER	General Ledger User, Progress S&L	03-JAN-22	-	Yes	2	Primary
38639	F10031	Dan Smith	bizdev@safepaas.com	Pending	03-JAN-2022 16:22	RENDERS	PRG_GENERAL_LEDGER_USER	General Ledger User, Progress S&L	03-JAN-22	-	Yes	3	Primary

Figure 14: *To the left is an example of the display screen that provides real time status to all self-service user-provisioning requests.*

- *In this workflow approvers receive notifications to approve or reject each user access request. The request includes the responsibilities requested as well as potential access risks based on the policies defined in the access management system.*
- *If the request is approved by all reviewers, the user access request is executed in Oracle E-Business Suite using standard security APIs to provision user and responsibility access.*
- *If an approver rejects the request and provides a comment, it's logged in the audit report and the information is sent back to the requester. An approver can grant a user request where the access risk is reported and "compensating" controls are implemented to mitigate the risk.*
- *For IT users that need emergency access to the production system, the approver may provide temporary access called "Firefighter" where all the activities are tracked and an audit trail is created to ensure compliance with access policies.*

SafePaaS™

Automated User provisioning considerations and benefits

- Standard user security administration tools available within enterprise applications are insufficient to mitigate the growing risk of fraud, financial misstatement and operational losses.
- Business Managers, Application Security Administrators and Auditors cannot rely on the standard user responsibilities assignment process where users are granted access without necessary policy checks and approvals.
- Automate and streamline the application access controls management by detecting user access risks in the existing ERP security model where users have access to sensitive or conflicting functions.
- Mitigate access risk by reconfiguring application roles that contain inherent risk. Reassign user roles so access is in compliance with company access policies.
- Prevent future policy violations by establishing an access request workflow where all new access requests are analyzed for policy violations and approvers make decisions based on access risks.

The preceding are best practices to remediate access risks and prevent recurrence in the future. However, most organizations must tolerate some level of access risks where the business resources are constrained. For example, in a small or remote business unit, you may have the same person enter and post journal entries.

In such cases you can deploy Continuous Controls Monitoring (CCM) to identify suspicious transactions, alert process owners when key application configurations are changed by "super users" and maintain audit trail over data changes such as customer credit limits, supplier bank accounts, etc. CCM is not covered here but should considered part of your compensating control strategy to manage overall access risks.

SafePaaS™