Safeguard your Business

with access controls that mitigate the risk of cyberthreats, financial misstatements and fraud in Oracle Applications

In this article, we will provide practical techniques to streamline user security management process with workflows that prevent security risks from user access requests. We will also cover audit analytics that detect Segregation of Duty (SoD) violations, data breaches, fraud, and other security risks.

Adil Khan, CEO, SafePaaS

Oracle Applications include security forms that are used to manually create, modify, and disable user accounts and their responsibilities across Oracle Applications. This standard user-responsibilities assignment process is inefficient and inconsistent where users are granted access without necessary policy checks and approvals. As the security risks are growing with the adoption of Cloud and Mobile, businesses are looking to streamline the user-provisioning process by consistently enforcing access policies (such as SoD rules) before violations get introduced into the ERP environment. This protects sensitive business information from potential threats and vulnerabilities.

We will share best practices to automate onboarding, offboarding and other administration user processes such as new hires, transfers, and promotions. We will also provide techniques to automatically aggregate and correlate identity data from HR, CRM, email systems and other "identity stores." You will also learn to streamline the user access certifications that are a critical requirement of many data security and privacy regulations, including UK Privacy Laws, US Sarbanes-Oxley, EU Directive and others. By regularly validating the appropriateness of user access privileges, your organisation can effectively meet audit and compliance requirements and improve its overall risk posture.

Application access risks

Application access risks are growing as organisations rapidly add users to their enterprise applications to execute all major business processes. Enterprise applications such as Oracle Cloud ERP, E-Business Suite, Peoplesoft and JD Edwards enable organisations to better engage and empower employees in the workplace, improve collaboration with business partners, and effectively manage customer relationships. However, ineffective access control within enterprise applications can result in operational losses, financial misstatements, and fraud.

Deficiencies in standard user access management

Managing user access to application entitlements has grown in complexity with the increase in functionality, transaction data and complexity of security configurations. The standard application access management tools to provision user security and maintain access controls over roles, responsibilities, and entitlement configurations no longer meet the access policy management needs. This can impede effective process enablement.

Business managers responsible for access controls often cannot obtain accurate function-mapped entitlement listings from enterprise applications, and thus have difficulty in building effective access controls to enforce SoD policies.

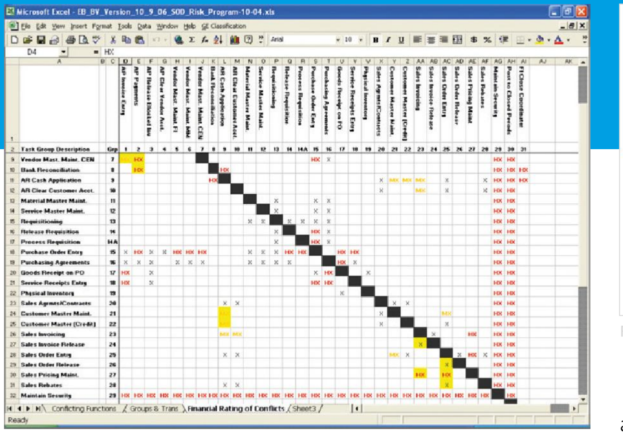
Access monitoring reports within the enterprise applications are not well designed to identify SoD violations, especially when it comes to policy-based user provisioning, cross-application SoD control monitoring, and ability to validate user access rights across disparate systems.

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 function level. They also do not consolidate detailed user activity logs unless those logs pertain to the administrators of the IDM. Consolidated activity logs which are critical for compliance reporting, auditing and forensics cannot be accomplished with IDM alone.

Mitigate risk of fraud, waste and errors with access controls

Organisations require Segregation of Duties access controls in ERP applications to mitigate the risk of fraud, waste and error. SoD is an internal control that prevents a single person from completing two or more tasks in a business process.

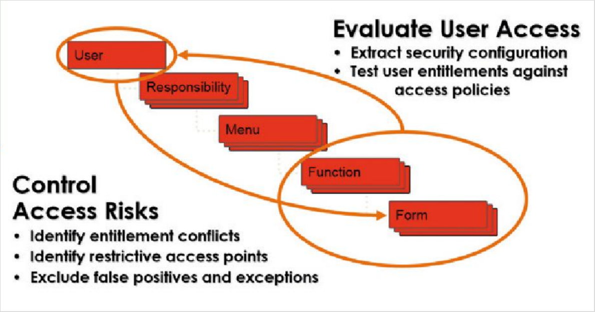
Actual job titles and organisational structures may vary greatly from one organisation to another, depending on the size and nature of the business. Therefore, it is important for management to analyse the skillset and capabilities of the individuals involved based on the likely risk and impact to business processes. Critical job duties can be categorised into four types of functions: authorisation, custody, record keeping, and reconciliation. In a perfect system, no one person should handle more than one type of function.


Microsoft Excel - EB_BV_Version_10_9_06_SOD_Risk_Program-10-04.xls
File Edit View Insert Format Tools Data Window Help GE Classification
Arial
10
Conflicting Functions
Groups & Trans
Financial Rating of Conflicts
Sheet3
Ready

D4 = HX

		AP Invoice Entry	AP Payments	AP Release Blocked Inv	AP Clear Vendor Acct.	Vendor Mast. Maint. FI	Vendor Mast. Maint. MM	Vendor Mast. Maint. CEN	Bank Reconciliation	AR Cash Application	AR Clear Customer Acct.	Material Master Maint.	Service Master Maint.	Requisitioning	Release Requisition	Process Requisition	Purchase Order Entry	Purchasing Agreements	Goods Receipt on PO	Service Receipts Entry	Physical Inventory	Sales Agrmts/Contracts	Customer Master Maint.	Customer Master (Credit)	Sales Invoicing	Sales Invoice Release	Sales Order Entry	Sales Order Release	Sales Pricing Maint	Sales Rebates	Maintain Security	Post to Closed Periods	FI Close Coordinator
Task Group Description	Grp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	14A	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Vendor Mast. Maint. CEN	7	MX	HX					■									HX	X													HX	HX	
Bank Reconciliation	8		HX						■	HX																					HX	HX	HX
AR Cash Application	9								HX	■												X	MX	MX	MX		X			X	HX	HX	HX
AR Clear Customer Acct.	10										■											X			MX		X			X	HX	HX	
Material Master Maint.	11											■		X			X	X													HX	HX	
Service Master Maint.	12												■	X			X	X													HX	HX	
Requisitioning	13											X	X	■	X	X	X	X													HX	HX	
Release Requisition	14													X	■		HX	X													HX	HX	
Process Requisition	14A													X		■	HX	X													HX	HX	
Purchase Order Entry	15	X	HX	X	X	HX	HX	HX				X	X	X	HX	HX	■		HX	HX											HX	HX	
Purchasing Agreements	16	X	X	X		X	X	X				X	X	X	X			■	HX	X											HX	HX	
Goods Receipt on PO	17	HX		X													X	HX	■		X										HX	HX	
Service Receipts Entry	18	HX		X													HX	HX		■											HX	HX	
Physical Inventory	19																		X		■										HX	HX	
Sales Agrmts/Contracts	20									X	X											■	X	X							HX	HX	
Customer Master Maint.	21									MX												X	■				MX				HX	HX	
Customer Master (Credit)	22									MX												X		■			X				HX	HX	
Sales Invoicing	23									MX	MX														■	X			HX		HX	HX	
Sales Invoice Release	24																								X	■					HX	HX	
Sales Order Entry	25									X	X												MX	X			■	X	HX	X	HX	HX	
Sales Order Release	26																										X	■			HX	HX	
Sales Pricing Maint.	27																								HX		HX		■		HX	HX	
Sales Rebates	28									X	X																X			■	HX	HX	
Maintain Security	29	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	■	HX	

FIGURE 1



Evaluate User Access

- Extract security configuration
- Test user entitlements against access policies

Control Access Risks

- Identify entitlement conflicts
- Identify restrictive access points
- Exclude false positives and exceptions

FIGURE 2

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)

Many companies find it challenging to implement effective SoD controls in their ERP systems, even though the concept of SoD is simple, as described above. To a large extent, this is due to the complexity and variety of the applications that automate key business processes. Also, the ownership and accountability for controlling those processes requires complete analysis of thousands of functions available across roles and responsibilities assigned to users. For example, to analyse 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. However, you must also exclude any false positives from the SoD control violation results that may occur as a result to overriding attributes, profiles, page level configurations or customisations that prevent such access.

Create access policies using the entitlements matrix

The Access Entitlement Matrix lists potential conflicts to determine what risk may be realised should a user have access or authorisation 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 even individual business unit. It is not uncommon for a large global company to have more than one matrix due to differences in the business processes by location or business unit. For example, a company may have a manufacturing business unit with a large amount of inventory, requiring a SoD matrix that focuses on specific inventory transactions. They may also have a service-based business unit necessitating a focus on project accounting, requiring a different SoD matrix. Though knowledge of similar businesses and industries can help to establish the entitlement conflict matrix, each business unit must perform a customised analysis of its conflicting transactions in order to capture the real risk for that particular business model. See Figure 1.

In this example, the matrix provides a financial risk rating of access roles called "responsibilities" in Oracle E-Business Suite that are assigned to a user. Each responsibility should be designed to mitigate the access control violation risks.
A responsibility design consists of menus, functions and options a user can access to process a transaction, change a setup or update a data object.

Ensure access policy compliance

To ensure compliance with access policies, you must test the security design to ensure that the responsibilities assigned to a user do not grant access to conflicting entitlements marked in the matrix. You can test access control effectiveness by extracting the security configuration from security tables and creating an access violation program that tests security configuration for violations of access policies defined in the entitlement matrix. The IT security team, with the approval of a remediation plan from business process owners, can correct and access violations by removing entitlements from users and roles. Auditors can use this "Access Violation" report to provide independent opinions regarding the effectiveness of access controls. Figure 2 shows how SoD rules are applied to the Oracle E-Business Suite security model.

Analyse access violations

Violations of access polices must be analysed to change user access assignments and correct application security configurations. You can start this analysis by examining the application function level access mapped in the rule sets that are tested in the relevant ERP security model. For example, vendor-update rights may be executed through a series of Responsibilities, Menus and Functions, "access points", within a Payables and Purchasing application. The presence of these access points assigned to specific users should be verified, walked through and documented in order to accurately verify a particular conflict. The challenge is that in most modern applications there is more than one way to execute the same transaction. For example, there may be ten ways to pay a vendor in a payables application, but the company may use only five of them. Moreover, the company is typically not aware of the other ten ways and usually does not restrict access to or control these other methods to execute a vendor payment.

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. Analysing all of the ways a user could potentially execute an application function is critical to accurate remediation and preventions of access risk.

User access management challenges

Today, organisations are challenged to ensure an effective and efficient access management process with a rapidly growing assortment of Cloud, on-premise and mobile applications. These challenges can result in management fatigue, materialised risk and operational losses:

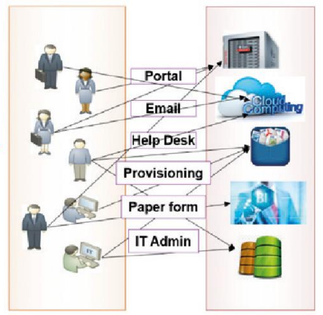
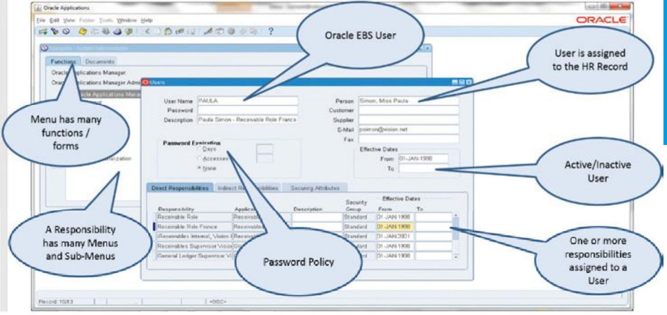


FIGURE 3


Oracle Applications
File Edit View Folder Tools Window Help
ORACLE
Functions
Documents
Users
Direct Responsibilities
Indirect Responsibilities
Securing Attributes
Oracle EBS User
User is assigned to the HR Record
Menu has many functions / forms
Active/Inactive User
A Responsibility has many Menus and Sub-Menus
Password Policy
One or more responsibilities assigned to a User

User Name: PAULA
Password:
Description: Paula Simon - Receivable Role France
Person: Simon, Miss Paula
Customer:
Supplier:
E-Mail: psimon@vision.net
Fax:
Effective Dates From: 01-JAN-1998 To:
Password Expiration: ○ Days ○ Accesses ● None

Responsibility	Application	Description	Security Group	From	To
Receivable Role	Receivable		Standard	01-JAN-1998	
Receivable Role France	Receivable		Standard	01-JAN-1998	
Receivables Internal, Vision	Receivable		Standard	01-JAN-2001	
Receivables Supervisor Vision	Gl		Standard	01-JAN-1998	
General Ledger Supervisor Vi			Standard	01-JAN-1998	

Record: 10/13

FIGURE 4

- User access requests, processed through various fragmented channels, without effective audit trails, waste time and money
- Lack of visibility into potential access policy violations during the request approval can compromise the security of enterprise applications and sensitive data such as financial statements, customer orders and supplier payments
- Companies can risk reputation with headline making security breaches, if security vulnerabilities in unprotected systems are exploited from outside or inside the company

User access request management

Many organisations process hundreds of users every day, adding, changing and deleting requests that are received through multiple sources including 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 because the approval request is granted without testing the security risks against policies at the granular functional level. Therefore, auditors cannot rely on the access controls and require management to manually test application access across disparate provisioning tools and workflow that consist of many human touch points including business managers, help desk, IT Security, etc, as shown in Figure 3.

Consequently, there are no consistent access policy enforcements within and across applications. Lack of common access controls and centralised audit trails increases the threat of data breach and cost of audits. IT security and management are burdened with time-consuming remediation tasks to ensure compliance with access policies.

User access assignment

User access assignment in ERP applications requires a security administrator to enter or update user details such as user ID, password, and associated employee information before assigning roles which entitle the user to access application functions and data. The standard application user assignment process is inefficient and inconsistent because this process does not prevent the security administrators from granting access to one or more roles that may violate an access policy.

For example, in Oracle E-Business Suite, when a user is assigned a responsibility using the standard security form available to the security administrator, there are no messages, warning or approval workflow generated if any of the functions available within a responsibility violate any access policy within the assigned responsibility or result in any SoD violation due to the combination of functions available to the user across responsibilities. The screenshot in Figure 4 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.

Access control deficiencies

Ineffective access request management across fragmented channels with limited audit trails, lack of visibility into potential access policy violations and mission critical systems are unprotected against data breach, fraud and financial misstatement risks. As a result, deficient application access controls are a common source of internal abuse and a top focus for IT audits. According to a recent Gartner survey, 44% of IT audit deficiencies are related to user access management. External audit firms are increasing focus on application access management testing as major regulations around the world require companies to comply with data privacy policies and ensure the effectiveness of internal control over financial statements. In a report published by Ernst & Young, 7 of the top 10 control deficiencies relate to user access control.

The following diagram shows the common access control deficiencies reported by auditors:

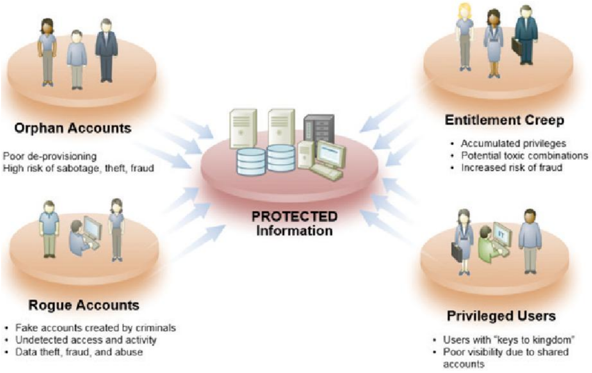

Orphan Accounts
Poor de-provisioning
High risk of sabotage, theft, fraud
Entitlement Creep
• Accumulated privileges
• Potential toxic combinations
• Increased risk of fraud
PROTECTED Information
Rogue Accounts
• Fake accounts created by criminals
• Undetected access and activity
• Data theft, fraud, and abuse
Privileged Users
• Users with "keys to kingdom"
• Poor visibility due to shared accounts

FIGURE 5

Automated access controls management

In this section, we will describe methods to automate and streamline the application access controls management process. We will provide examples to:

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

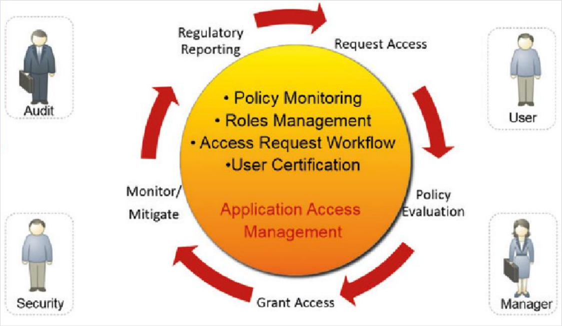


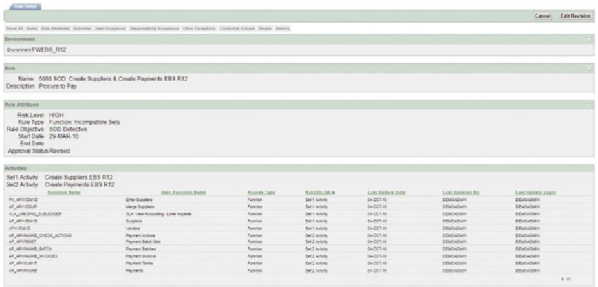
FIGURE 6

Figure 6 shows the complete access controls management life-cycle.

Monitor policy compliance

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

The following screenshot shows a SoD rule to detect user access violations where a user can Create Supplier and Create a Payment for that Supplier.



Environment

Environment FWEBS_R12

Rule

Name 5980 SOD: Create Suppliers & Create Payments EBS R12
Description Procure to Pay

Rule Attributes

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

Activities

Set1 Activity Create Suppliers EBS R12
Set2 Activity Create Payments EBS R12

Function Name	User Function Name	Access Type	Activity Set	Last Update Date	Last Updated By	Last Update Login
FA_APXVDMVD	Enter Suppliers	Function	Set 1 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
AP_APXVDDUP	Merge Suppliers	Function	Set 1 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
XLA_LINESINQ_SUBLEDGER	SLA: View Accounting - Lines Inquiries	Function	Set 1 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
AP_APXVDMVD	Suppliers	Function	Set 1 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
APXVDMVD	Vendors	Function	Set 1 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
AP_APXPAWKB_CHECK_ACTIONS	Payment Actions	Function	Set 2 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
AP_APXPBSET	Payment Batch Sets	Function	Set 2 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
AP_APXPAWKB_BATCH	Payment Batches	Function	Set 2 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
AP_APXPAWKB_INVOICES	Payment Invoices	Function	Set 2 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
AP_APXSUMVT	Payment Terms	Function	Set 2 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN
AP_APXPAWKB	Payments	Function	Set 2 Activity	04-OCT-16	DEMOADMIN	DEMOADMIN

1 - 11

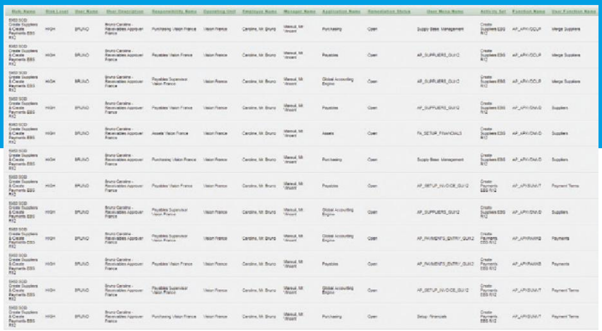
FIGURE 7

You will note that there are five functions in Oracle to create suppliers and six functions to pay suppliers. The grouping of functions into business actives enables business managers and application security administrators to assess the business risk as well as make technical configuration changes to remediate it.

Once the rules are created, you can run the access violations program that test the rule against a "snapshot" of the ERP security tables where the user and responsibilities do not comply with the policy. The results can be viewed in an access policy violations report.

For example, the report in Figure 8 shows that a user named Bruno has the potential access risk of creating a supplier and paying that supplier.

Notice that the report shows the responsibilities, menus and functions in each row that enable the user to access the business activities in conflict. Also, we can expedite the remediation actions by reporting the organisation, Vision France, and the name of Bruno's manager, Mr. Mareul Vincent from the HR table.



Rule Name	Risk Level	User Name	User Description	Responsibility Name	Operating Unit	Employee Name	Manager Name	Application Name	Remediation Status	User Menu Name	Activity Set	Function Name	User Function Name
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Purchasing Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Purchasing	Open	Supply Base Management	Create Suppliers EBS R12	AP_APXVDDUP	Merge Suppliers
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Payables Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Payables	Open	AP_SUPPLIERS_GUI12	Create Suppliers EBS R12	AP_APXVDDUP	Merge Suppliers
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Payables Supervisor Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Global Accounting Engine	Open	AP_SUPPLIERS_GUI12	Create Suppliers EBS R12	AP_APXVDDUP	Merge Suppliers
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Payables Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Payables	Open	AP_SUPPLIERS_GUI12	Create Suppliers EBS R12	AP_APXVDMVD	Suppliers
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Assets Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Assets	Open	FA_SETUP_FINANCIALS	Create Suppliers EBS R12	AP_APXVDMVD	Suppliers
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Purchasing Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Purchasing	Open	Supply Base Management	Create Suppliers EBS R12	AP_APXVDMVD	Suppliers
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Payables Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Payables	Open	AP_SETUP_INVOICE_GUI12	Create Payments EBS R12	AP_APXSUMVT	Payment Terms
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Payables Supervisor Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Global Accounting Engine	Open	AP_SUPPLIERS_GUI12	Create Suppliers EBS R12	AP_APXVDMVD	Suppliers
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Payables Supervisor Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Global Accounting Engine	Open	AP_PAYMENTS_ENTRY_GUI12	Create Payments EBS R12	AP_APXPAWKB	Payments
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Payables Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Payables	Open	AP_PAYMENTS_ENTRY_GUI12	Create Payments EBS R12	AP_APXPAWKB	Payments
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Payables Supervisor Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Global Accounting Engine	Open	AP_SETUP_INVOICE_GUI12	Create Payments EBS R12	AP_APXSUMVT	Payment Terms
5980 SOD: Create Suppliers & Create Payments EBS R12	HIGH	BRUNO	Bruno Caroline - Receivables Approver France	Purchasing Vision France	Vision France	Caroline, Mr. Bruno	Mareul, Mr Vincent	Purchasing	Open	Setup: Financials	Create Payments EBS R12	AP_APXSUMVT	Payment Terms

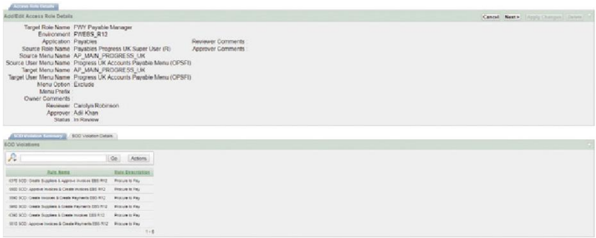
FIGURE 8

Remediate control defects

Access risk remediation requires two major types of corrective actions. Firstly, updating the security configuration in the application roles that pose "inherent" risk by enabling the user to access conflicting entitlements within a single role. Secondly, reassigning user roles where the violation is caused by the user having access two or more conflicting roles.

User role security configuration is the root cause for the majority of access policy violations. However, updating roles in a production ERP system with hundreds or even thousands of active users can negatively impact business performance. Many companies and their auditors get bogged down during remediation because of the difficulty in changing security design while business users need to perform their task. Therefore, we recommend automating the role redesign process by analysing the source roles with violations and creating "target" roles that can be reconfigured and tested for access policy compliance in a simulated environment before deploying the compliant roles into the production system.

For example, the following image shows a new target role "FWY Payable Manager" that is derived from the source role "Payables Progress UK Super User" in Oracle E-Business Suite:



Add/Edit Access Role Details

Target Role Name FWY Payable Manager
Environment FWEBS_R12
Application Payables
Source Role Name Payables Progress UK Super User (R)
Source Menu Name AP_MAIN_PROGRESS_UK
Source User Menu Name Progress UK Accounts Payable Menu (OPSFI)
Target Menu Name AP_MAIN_PROGRESS_UK
Target User Menu Name Progress UK Accounts Payable Menu (OPSFI)
Menu Option Exclude
Menu Prefix
Owner Comments
Reviewer Carolyn Robinson
Approver Adil Khan
Status In Review

Reviewer Comments
Approver Comments

SOD Violations

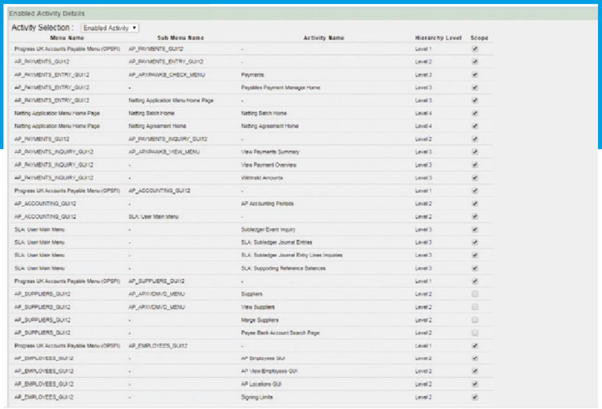
Rule Name	Rule Description
4370 SOD: Create Suppliers & Approve Invoices EBS R12	Procure to Pay
5900 SOD: Approve Invoices & Create Invoices EBS R12	Procure to Pay
5990 SOD: Create Invoices & Create Payments EBS R12	Procure to Pay
5980 SOD: Create Suppliers & Create Payments EBS R12	Procure to Pay
4360 SOD: Create Suppliers & Create Invoices EBS R12	Procure to Pay
5010 SOD: Approve Invoices & Create Payments EBS R12	Procure to Pay

1 - 6

FIGURE 9

You will note that this role has a number of SoD access policy violations including "Create Supplier and Create Payments". Let's say that we want to remove the Create Supplier entitlement to correct the security configuration in the target role. We can use the exclusion method available in Oracle User Security Form to exclude all the functions associated with the Create Supplier entitlement. The following page shows that we can simply check off the supplier functions in Figure 10.

Once the configuration is saved, this program simulates the access policy test to ensure that the target role is compliant with the policy. The program also generates the LDT file that can be loaded directly into EBS using the standard FNDLOAD program, without impacting the user in the production system and saving costly administration activities.



Enabled Activity Details

Activity Selection : Enabled Activity ▾

Menu Name	Sub Menu Name	Activity Name	Hierarchy Level	Scope
Progress UK Accounts Payable Menu (OPSFI)	AP_PAYMENTS_GUI12	-	Level 1	☑
AP_PAYMENTS_GUI12	AP_PAYMENTS_ENTRY_GUI12	-	Level 2	☑
AP_PAYMENTS_ENTRY_GUI12	AP_APXPAWKB_CHECK_MENU	Payments	Level 3	☑
AP_PAYMENTS_ENTRY_GUI12	-	Payables Payment Manager Home	Level 3	☑
AP_PAYMENTS_ENTRY_GUI12	Netting Application Menu Home Page	-	Level 3	☑
Netting Application Menu Home Page	Netting Batch Home	Netting Batch Home	Level 4	☑
Netting Application Menu Home Page	Netting Agreement Home	Netting Agreement Home	Level 4	☑
AP_PAYMENTS_GUI12	AP_PAYMENTS_INQUIRY_GUI12	-	Level 2	☑
AP_PAYMENTS_INQUIRY_GUI12	AP_APXPAWKB_VIEW_MENU	View Payments Summary	Level 3	☑
AP_PAYMENTS_INQUIRY_GUI12	-	View Payment Overview	Level 3	☑
AP_PAYMENTS_INQUIRY_GUI12	-	Withheld Amounts	Level 3	☑
Progress UK Accounts Payable Menu (OPSFI)	AP_ACCOUNTING_GUI12	-	Level 1	☑
AP_ACCOUNTING_GUI12	-	AP Accounting Periods	Level 2	☑
AP_ACCOUNTING_GUI12	SLA: User Main Menu	-	Level 2	☑
SLA: User Main Menu	-	Subledger Event Inquiry	Level 3	☑
SLA: User Main Menu	-	SLA: Subledger Journal Entries	Level 3	☑
SLA: User Main Menu	-	SLA: Subledger Journal Entry Lines Inquiries	Level 3	☑
SLA: User Main Menu	-	SLA: Supporting Reference Balances	Level 3	☑
Progress UK Accounts Payable Menu (OPSFI)	AP_SUPPLIERS_GUI12	-	Level 1	☑
AP_SUPPLIERS_GUI12	AP_APXVDMVD_MENU	Suppliers	Level 2	☐
AP_SUPPLIERS_GUI12	AP_APXVDMVD_MENU	View Suppliers	Level 2	☐
AP_SUPPLIERS_GUI12	-	Merge Suppliers	Level 2	☐
AP_SUPPLIERS_GUI12	-	Payee Bank Account Search Page	Level 2	☐
Progress UK Accounts Payable Menu (OPSFI)	AP_EMPLOYEES_GUI12	-	Level 1	☑
AP_EMPLOYEES_GUI12	-	AP Employees GUI	Level 2	☑
AP_EMPLOYEES_GUI12	-	AP View Employees GUI	Level 2	☑
AP_EMPLOYEES_GUI12	-	AP Locations GUI	Level 2	☑
AP_EMPLOYEES_GUI12	-	Signing Limits	Level 2	☑

FIGURE 10

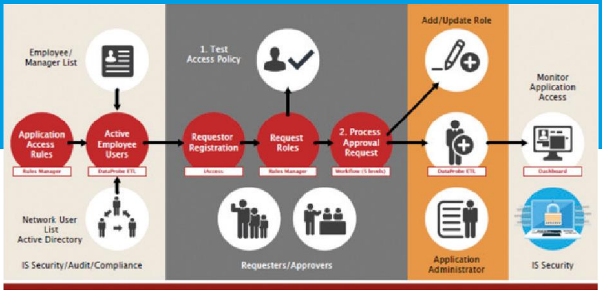


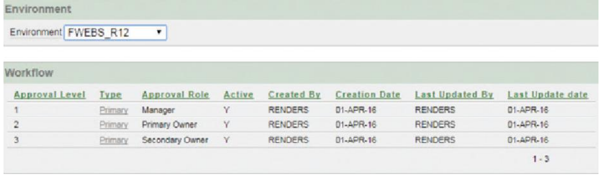
FIGURE 11

Provision users with policy compliance

Once you have detected and remediated the user access violations in your product ERP system, it is important to prevent the violations from recurring as new user requests are processed and the security model is updated to meet new business requirements. Otherwise, all your effort will have to be repeated in the next audit cycle, if the users' role assignments are changed without testing for access policy impact.

The swim-lane diagram in Figure 11, shows the key activities by business roles that are required to support self-service user provisioning process to ensure compliance with access policies.

The first step in setting up a user access request workflow is to determine the approval levels and roles. In Figure 12, we have set up three levels of approval so that the employee's manager is the first approver. The manager information is obtained from the HR tables as part of the ERP security "snapshot" that is processed at the frequency defined by management. After the manager approval, the approval request goes to a primary and a secondary approver as well. The primary approver can be a "functional" manager most familiar with the functions available in the requested Oracle Responsibility. A technical manager with the understanding of the Oracle security model may be assigned the approval responsibility as a secondary approver. See approver workflow setup below:



Environment

Environment FWEBS_R12 ▾

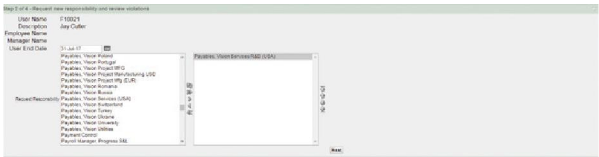
Workflow

Approval Level	Type	Approval Role	Active	Created By	Creation Date	Last Updated By	Last Update date
1	Primary	Manager	Y	RENDERS	01-APR-16	RENDERS	01-APR-16
2	Primary	Primary Owner	Y	RENDERS	01-APR-16	RENDERS	01-APR-16
3	Primary	Secondary Owner	Y	RENDERS	01-APR-16	RENDERS	01-APR-16

1 - 3

FIGURE 12

Once the workflow is configured and the approvers are assigned to active Oracle E-Business Suite responsibilities, a registered user can use the access request page to access new responsibilities. The following image shows a user that is requesting the Payables Vision services R&D (USA) responsibility:



Step 2 of 4 - Request new responsibility and review violations

User Name F10021
Description Jay Cutler
Employee Name
Manager Name
User End Date 31-Jul-17

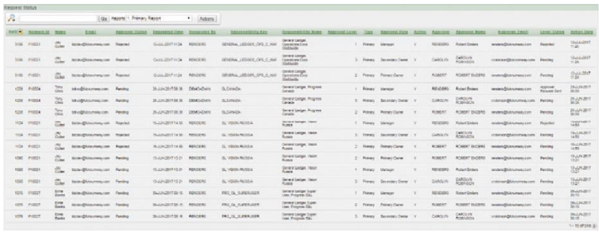
Request Responsibility:
Payables, Vision Poland
Payables, Vision Portugal
Payables, Vision Project MFG
Payables, Vision Project Manufacturing USD
Payables, Vision Project Mfg (EUR)
Payables, Vision Romania
Payables, Vision Russia
Payables, Vision Services (USA)
Payables, Vision Switzerland
Payables, Vision Turkey
Payables, Vision Ukraine
Payables, Vision University
Payables, Vision Utilities
Payment Control
Payroll Manager, Progress S&L

Payables, Vision Services R&D (USA)

Next

FIGURE 13

Once the user submits the access request, it is routed by the pre-configured workflow to each person assigned the approval role in the workflow. The IS Security Administrator can monitor all access requests and change or cancel a request if required. The following report shows an example of the display screen that provide real time status to all self-service user-provisioning requests:



Request Status

Go Reports 1. Primary Report ▾ Actions

FIGURE 14

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

The pages and report in the examples above are created using Oracle APEX application available on SafePaaS.

Conclusion

The standard user security administration tools available within enterprise applications are no longer sufficient to mitigate the growing risk of fraud, financial misstatement and operational losses. Business Managers, Application Security Administrators, and Auditors can't rely on the standard user responsibilities assignment process where users are granted access without necessary policy checks and approvals.

You can automate and streamline the application access controls management process by detecting user access risks in the existing ERP security model where the users have access to sensitive or conflicting functions. The access risk can be mitigated by reconfiguring the application roles that contain inherent access risk. In addition, you can reassign user roles where combined entitlements across all the roles, assigned to a user, are in compliance with your company's access policies. After remediation of access risks, it's important to prevent any future access policy violations by establishing an access request workflow where all new access requests are analysed for policy violations and approvers can make decisions based on the access risks before a user is granted access to new application privileges.

In this article, we have provided the best practices to remediate access risks and prevent recurrence in the future. However, we also recognise that most organisations must tolerate some level of access risks where the business resources are constrained. For example, in a small 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 changes by "super users" and maintain audit trail over data changes such as customer credit limits, supplier bank accounts, etc. We did not cover CCM here, but you should consider it as part of your compensating control strategy to manage overall access risks. ■

ABOUT THE AUTHOR

Adil Khan
CEO, SafePaaS

Adil Khan is the CEO at SafePaaS, a firm specialising in Governance, Risk and Compliance solutions with over 250 customers in the Americas, EMEA and Asia Pacific. Adil has authored "Governance, Risk and Compliance Handbook for Oracle Applications" and he serves on the board of the Oracle Applications Users Group (OAUG) GRC Special Interest Group. He has given over fifty presentations on GRC trends, best practices and case studies at many industry conferences including Gartner GRC Summit, IIA, ISACA, Collaborate, UKOUG and Oracle OpenWorld.