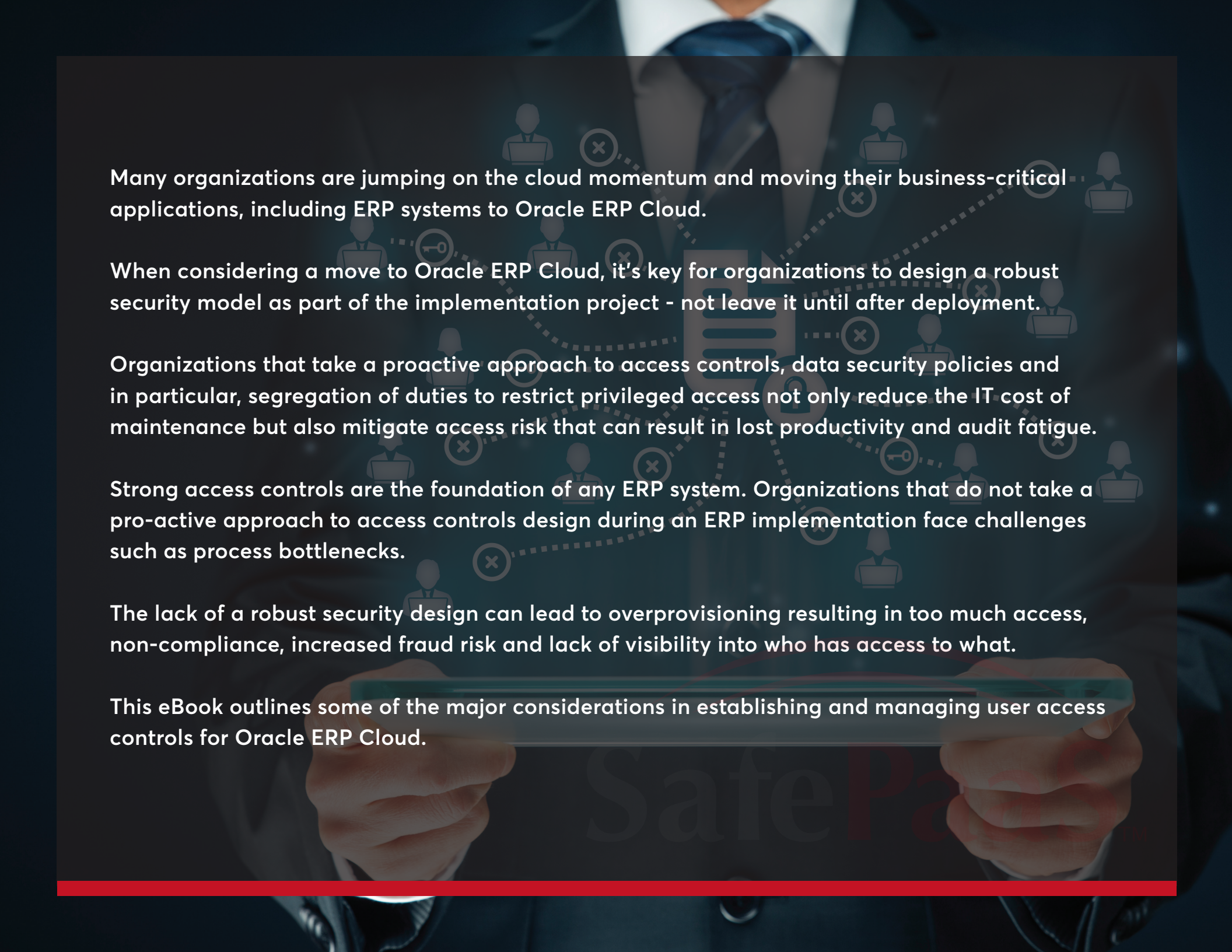




Secure Oracle ERP Cloud with Effective Access Controls





Many organizations are jumping on the cloud momentum and moving their business-critical applications, including ERP systems to Oracle ERP Cloud.

When considering a move to Oracle ERP Cloud, it's key for organizations to design a robust security model as part of the implementation project - not leave it until after deployment.

Organizations that take a proactive approach to access controls, data security policies and in particular, segregation of duties to restrict privileged access not only reduce the IT cost of maintenance but also mitigate access risk that can result in lost productivity and audit fatigue.

Strong access controls are the foundation of any ERP system. Organizations that do not take a pro-active approach to access controls design during an ERP implementation face challenges such as process bottlenecks.

The lack of a robust security design can lead to overprovisioning resulting in too much access, non-compliance, increased fraud risk and lack of visibility into who has access to what.

This eBook outlines some of the major considerations in establishing and managing user access controls for Oracle ERP Cloud.

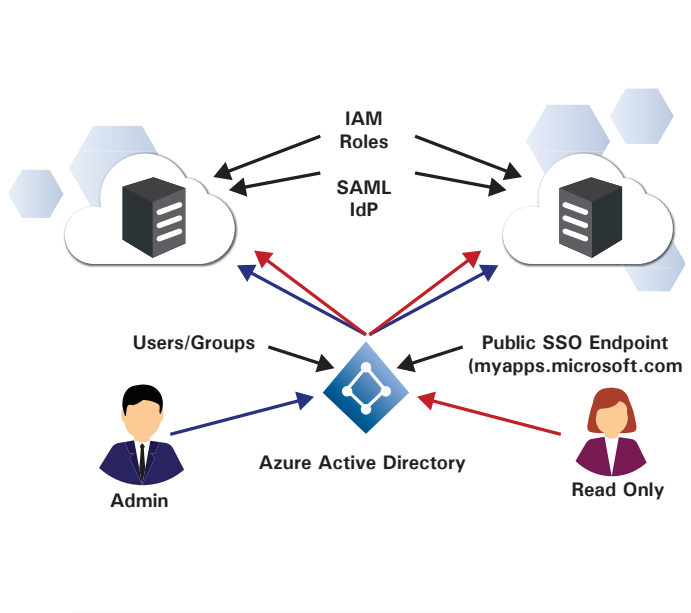
Security Risks in Oracle ERP Cloud

- Standard user security administration tools within Oracle enterprise applications are insufficient to detect Segregation of Duties risks that can result in fraud, financial misstatement and operational losses. Specialized policy-based advanced analytics is required to enforce effective access controls that can prevent users from executing conflicting transactions within a business process.
- Seeded roles in Oracle ERP Cloud come with inherent segregation of duties risk.
- Organizations are not static. People come and go, move departments, change roles. This is when overprovisioning occurs and people are given more access than they really need to perform their job.
- Managers responsible for periodically certifying user access often cannot obtain accurate and timely user to role assignment details, creating difficulty in monitoring and certifying user access to privileges, transactions, configurations and master data.
- Oracle ERP Cloud as well as third-party IT tools lack policy-based access control in the provisioning process which can result in access policy violations and elevated security risks to privileged data stored in the cloud.

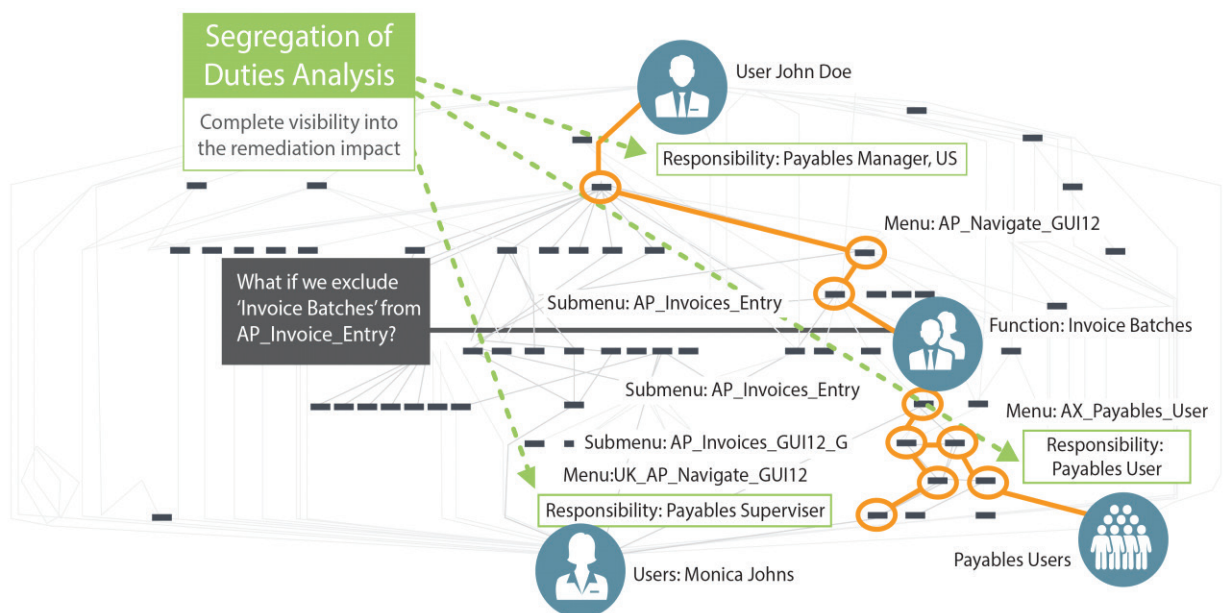
Provisioning Systems do not detect or prevent user access requests

User Access Provisioning tools such as Identity Management (IDM) and IT Service Management (ITSM) systems operate at such a high level that they cannot detect the risks in the fine-grained privileges requested by the user through abstract roles catalogued in these tools. Traditional Identity and Access Management solutions control user access to enterprise systems by provisioning roles from a catalog of high level abstract roles, that do not prevent user ability to access sensitive data, or privileges, resulting in significant audit findings, increased risk of regulatory penalties and costly remediation effort.

Traditional IAM



IAM with Fine Grained IGA



Access Controls Implementation Approach

Organizations require Segregation of Duties 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.

For example, to analyze the SoD risk that enables users in Oracle ERP Cloud to create a supplier and pay that supplier, you must identify all privileges assigned to the user that constitute the entitlements granted through one or more roles such as Payables Manager, Purchasing Manager, etc.

SoD Analysis requires Oracle Cloud ERP security design skill-set and enterprise risk management expertise to define policies in terms of fine-grained privileges that represent the potential risk and impact to key business processes. Business Process Owners responsible for maintaining SoD controls are requested to categorize critical job duties into four types of privileges: authorization, custody, record keeping, and reconciliation. No one person should perform more than one type of privilege within the same business process.



Risk Managers often use 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)

Define Access Policies using the Entitlements Matrix

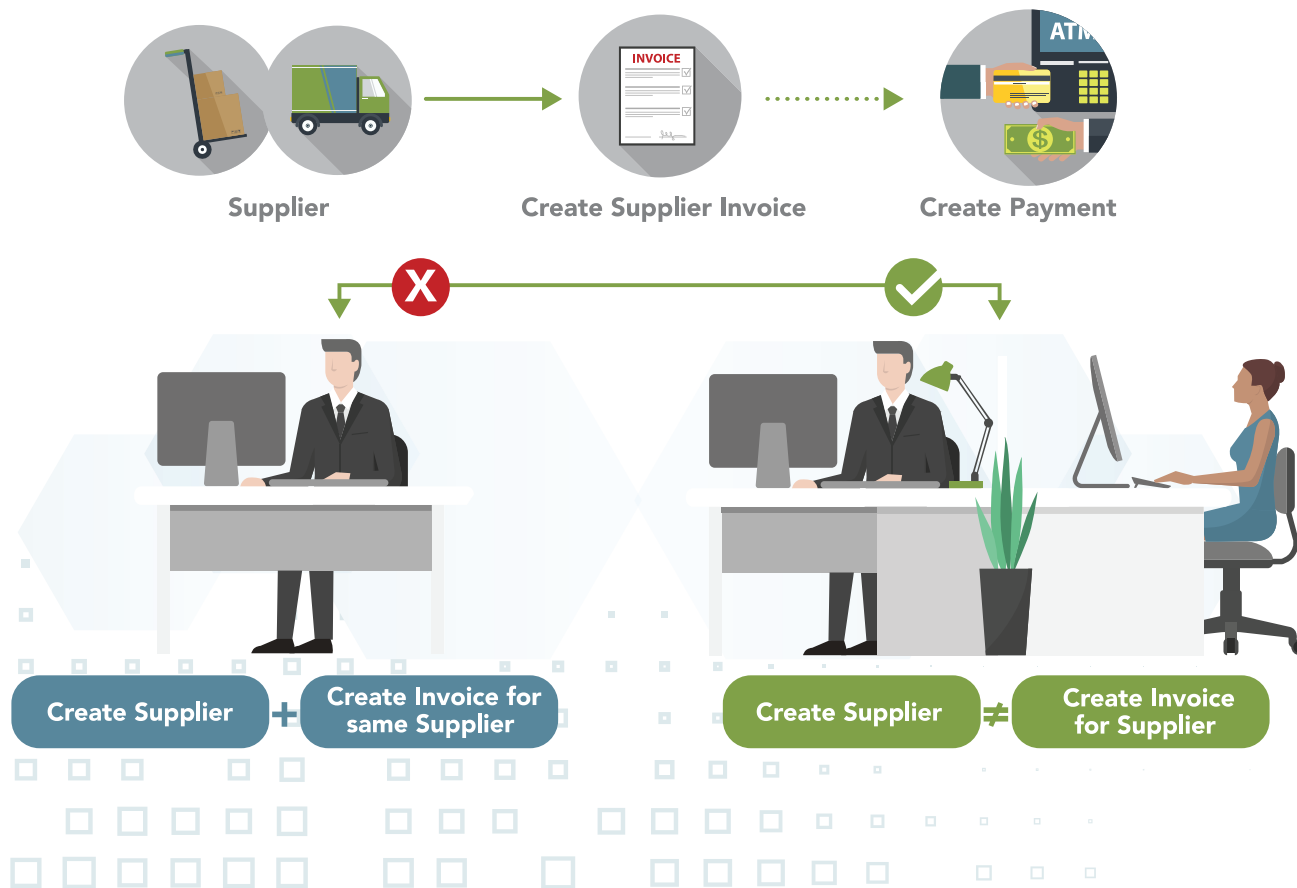
The entitlement matrix has been devised and used by many organizations as a method to determine access risks specific to an organization's ERP user security model. The following diagram is an example of an entitlement matrix:

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 to capture the real risk for that particular business model.
- The matrix provides a financial risk rating of access roles called “privileges” in Oracle ERP Cloud that are assigned to a user specifying with business privileges available to them through the role.
- Ideally, each role should be designed to mitigate access control violation risks. A role design consists of privileges and options a user can access to process business transactions and change data.
- The matrix comprises of the valid high-risk roles that are aligned on both the X and Y axis, where the intersection between two roles are marked to indicate the level of risk associated when an individual is given the requisite roles.

Ensure User Roles Comply with Access Policies

- It is important to test the security design to ensure that roles granted to users do not grant access to conflicting permissions causing SoD violations.
- Periodically test access control effectiveness by extracting the role configuration from application security reports. This will provide the foundation to create an access violation process that tests security configuration for violations of access policies.
- The Application security administrator should correct access violations by removing permissions from users and roles.
- Auditors would review the roles compliance report to provide independent opinions regarding the effectiveness of access controls.

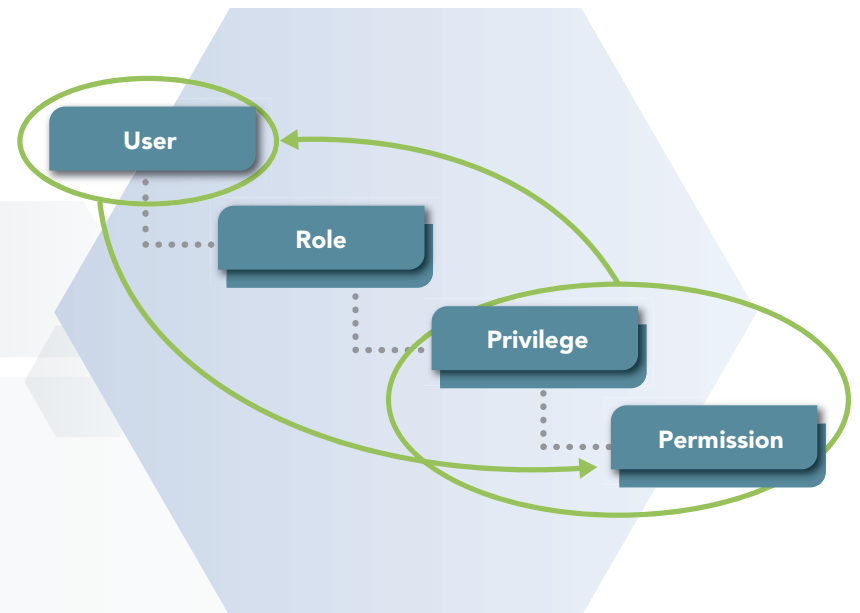


Evaluating User Access Assignments to Application Roles

Evaluating user access is a critical activity to minimize risk and comply with the organization's access policies. It is necessary to understand all the roles, privileges and other security attributes that grant user access to perform process activities. Any violations detected during this evaluation step, require the security administrator to make the necessary remediation recommendations and address the known incidents.

This diagram is an example of user security model access structure in Oracle ERP Cloud. The Oracle ERP Cloud security model is flexible however, given the complexity of the design it's essential to design and build security in the implementation phase to ensure effective segregation of duties.

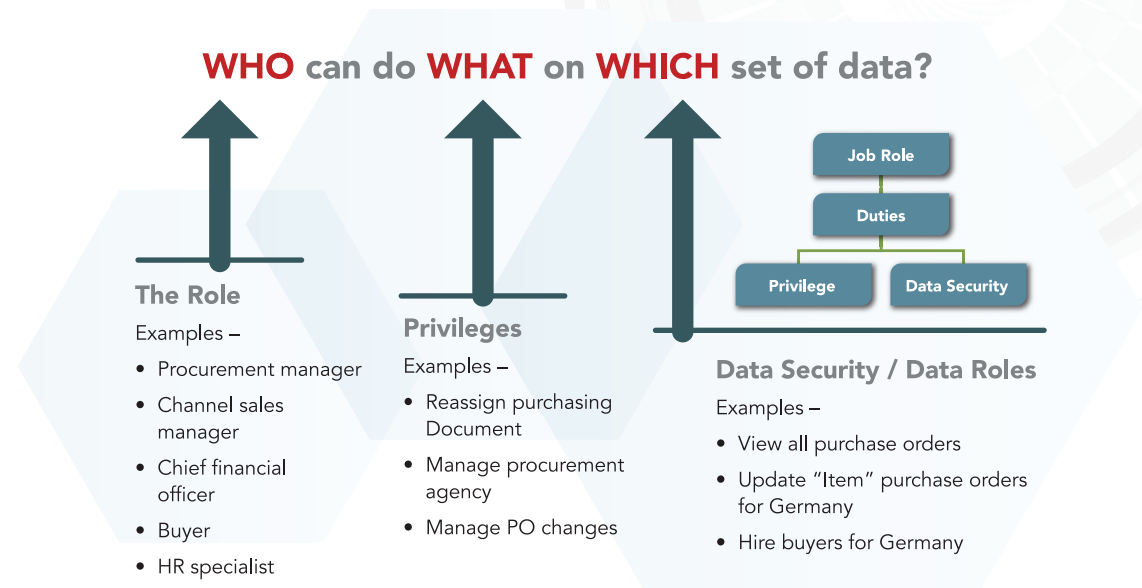
Oracle Fusion security is based on role-based access security. The role-based security model also called role based access control, (in short, RBAC) is a way of restricting system access to the users. A user should not be able to have access to complete systems or information.



Analyze Access Violations

- Violations of access policies 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 privilege'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 Role privileges within the Payables and Purchasing applications.
- The privileges assigned to specific users should be verified, walked through and documented to accurately verify a particular conflict.

The security model diagram on p. 8 shows how SoD rules are applied to the Oracle ERP Cloud security model.



Risks in Controlling User Access Requests

Once you have detected and remediated existing risk in your business applications, you must prevent future risks introduced through user access requests.

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 privilege is critical to accurate remediation and prevention of access risk.
- Users are provided multiple roles providing multiple access paths to the same transaction.
- Remediation through changing roles has 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 to understand the full potential for fraud, not just the limited view of the known methods.

Organizations are challenged to ensure an effective and efficient access management process with a growing assortment of Cloud, on-premise and mobile applications.

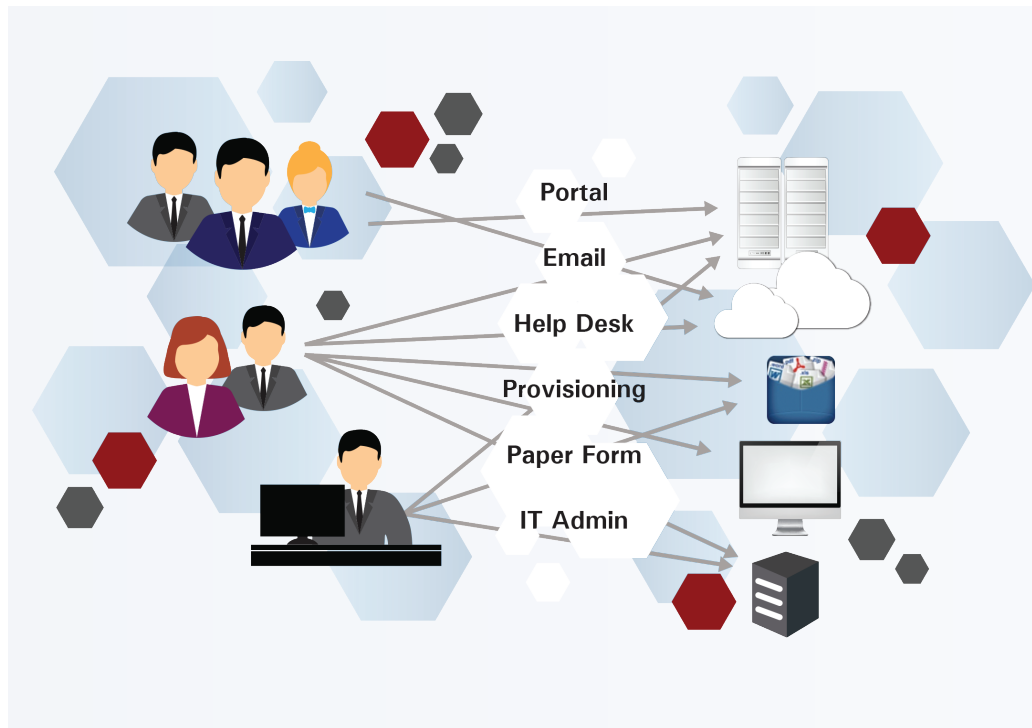
These challenges can result in management fatigue, materialized risk and operational losses in the following areas:

- User access requests are manually processed through various fragmented channels and ERPs, have no effective audit trails, and 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 causing unknown access risk during the provisioning process.

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.

Access risks created by multiple and conflicting authorities:



- As shown in this diagram, 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 policies.
- Approval request is granted without testing the security risks against policies at the privilege 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.

User Access Governance Limitations in Oracle Cloud ERP

The following points identify 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.

User Account Details: SafePaas1

User Information: User Category: DEFAULT, User Name: SafePaas1, First Name: SafePaas1, Last Name: SafePaas1, Email: SafePaas1@...
 Account Information: Password Expiration Date: 02/16/2022, Active: [X], Locked: []
 Roles: Application Implementation Consultant, IT Security Manager
 Role Code: ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB, ORA_FND_IT_SECURITY_MANAGER_JOB
 Assignable: No, No
 Auto-Provisioned: No, No

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.

The screenshot of the Oracle ERP Cloud Security Form shows all the direct, as well as indirect, user security and privilege assignment attributes granted without any preventive policy enforcement.

Roles: Search: Job roles:Duty roles:Abstract roles:DEI... Application Implementation Consultant
 Expand Toward: Privileges
 Role Name: Student Party View, Order Orchestration Administration, PSC Delete Plan Review Comments addde, SOA Operator Role, PSC Print Appeal Letter, Public Sector Agency Receipts Transac..., Application World Reference Administration, BPM Composer Deployer Role
 Role Code: ORA_HEY_STUDENT_PARTY_VIEW_D..., ORA_DOO_ORDER_ORCHESTRATION..., ORA_PSC_DELETE_PLAN_REVIEW_C..., SOAOperator, ORA_PSC_PRINT_APPEAL_LETTER_D..., FBI_PUBLIC_SECTOR_AGENCY_RECE..., ORA_FND_APP_WORLD_REFERENCE..., BPMComposerDeployer
 Inherited by Role Name: Student Party Maintenance, Supply Chain Application Administrator, PSC Manage Plan Review Cycles in Plan..., Supply Chain Application Administrator, PSC Code Enforcement Application Admi..., PSC Building Inspector, Higher Education Application Administrator, Customer Relationship Management Appl...

Manage Data Access for Users

Security Context: Data access set

* User Name: SafePaas1, Role: []

Search Results:

User Name	Role	Security Context	Security Context Value
SafePaas1	Application Implementation Consultant	Data access set	
SafePaas1	IT Security Manager	Data access set	

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.

This diagram shows the common access control deficiencies reported by auditors:



Best practices for Controlling Access Risks in User Access Requests

There are well established best practices to automate and streamline the application access controls management process.

Doing so enables an organization to:

- Monitor access policies with user and role violation reports.
- Manage access roles to remediate violations by excluding privileges from 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 roles.
- Certify user access to assigned roles by notifying the manager of user access and capturing information to disable access that is no longer required.

This diagram shows the common access control deficiencies reported by auditors:



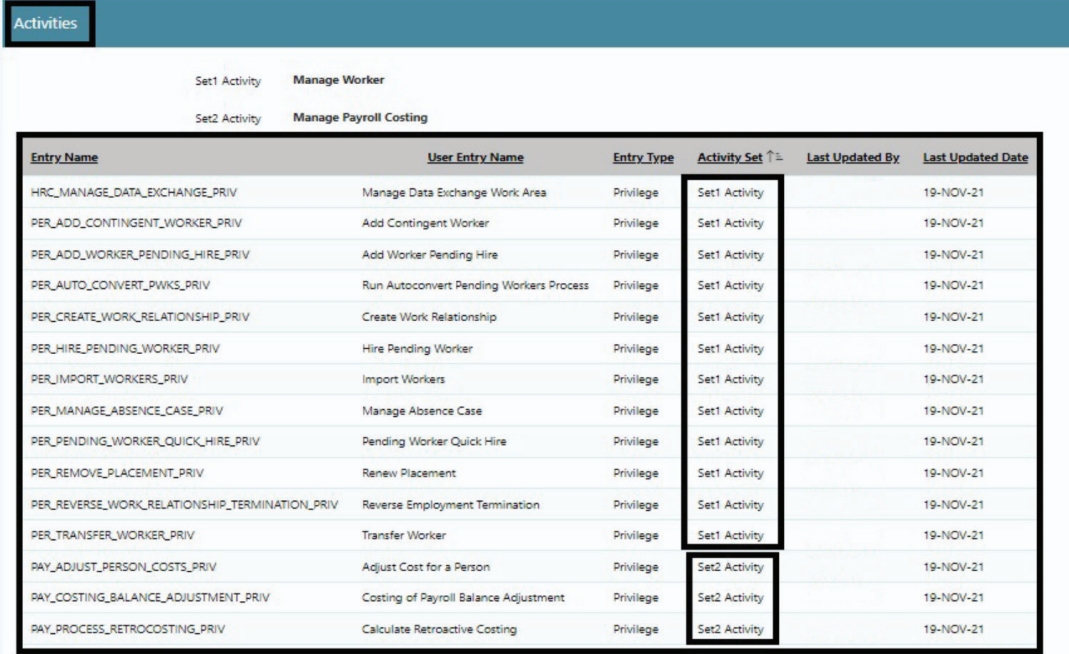
Automating User Access Management

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 SafePaaS activities are assigned to users through roles which enable the user to access privileges.
- To monitor policy compliance, you must define privileges that enable business activities.

The screenshot below shows a SoD rule in SafePaaS for Oracle ERP Cloud.



The screenshot displays the 'Activities' section of the SafePaaS interface. It shows two activity sets: 'Set1 Activity: Manage Worker' and 'Set2 Activity: Manage Payroll Costing'. Below these, a table lists various activities and their associated privileges. A red box highlights the 'Activity Set' column, which shows that activities are grouped into Set1 and Set2.

Entry Name	User Entry Name	Entry Type	Activity Set	Last Updated By	Last Updated Date
HRC_MANAGE_DATA_EXCHANGE_PRIV	Manage Data Exchange Work Area	Privilege	Set1 Activity		19-NOV-21
PER_ADD_CONTINGENT_WORKER_PRIV	Add Contingent Worker	Privilege	Set1 Activity		19-NOV-21
PER_ADD_WORKER_PENDING_HIRE_PRIV	Add Worker Pending Hire	Privilege	Set1 Activity		19-NOV-21
PER_AUTO_CONVERT_PWKS_PRIV	Run Autoconvert Pending Workers Process	Privilege	Set1 Activity		19-NOV-21
PER_CREATE_WORK_RELATIONSHIP_PRIV	Create Work Relationship	Privilege	Set1 Activity		19-NOV-21
PER_HIRE_PENDING_WORKER_PRIV	Hire Pending Worker	Privilege	Set1 Activity		19-NOV-21
PER_IMPORT_WORKERS_PRIV	Import Workers	Privilege	Set1 Activity		19-NOV-21
PER_MANAGE_ABSENCE_CASE_PRIV	Manage Absence Case	Privilege	Set1 Activity		19-NOV-21
PER_PENDING_WORKER_QUICK_HIRE_PRIV	Pending Worker Quick Hire	Privilege	Set1 Activity		19-NOV-21
PER_REMOVE_PLACEMENT_PRIV	Renew Placement	Privilege	Set1 Activity		19-NOV-21
PER_REVERSE_WORK_RELATIONSHIP_TERMINATION_PRIV	Reverse Employment Termination	Privilege	Set1 Activity		19-NOV-21
PER_TRANSFER_WORKER_PRIV	Transfer Worker	Privilege	Set1 Activity		19-NOV-21
PAY_ADJUST_PERSON_COSTS_PRIV	Adjust Cost for a Person	Privilege	Set2 Activity		19-NOV-21
PAY_COSTING_BALANCE_ADJUSTMENT_PRIV	Costing of Payroll Balance Adjustment	Privilege	Set2 Activity		19-NOV-21
PAY_PROCESS_RETROCASTING_PRIV	Calculate Retroactive Costing	Privilege	Set2 Activity		19-NOV-21

Assessing Risks in Oracle ERP Cloud

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

- There are five privileges in Oracle to create suppliers and six privileges to pay suppliers.
- The grouping of privileges 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 roles do not comply with policy. The results can be viewed in an access policy violations report.

This screenshot shows that a user has the potential access risk of creating a supplier and paying that supplier. The report shows the roles, and privileges in each row that allow the user to access conflicting business activities.

Select	Rule Name	Start Entry Name	Violation Entry	Violation Entry Name	Violation Entry Description	Violation Status	Rule Type	Compas Id	Group Id	Rule activity version	User Id	Start entry Id	Child entry Id	Exception score
<input type="checkbox"/>	Manage Employee and Manage Compensation	Application Implementation Consultant[DRA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB]	Privilege	CMR_MANAGE_COMPENSATION_PLAN_DEFINITION_PRIV	Manage Compensation Plan Definition	OPEN	SET	\$0461	1925	2	32081343	1257557943	1257569391	-
<input type="checkbox"/>	Manage Compensation and Manage Payroll Batch Process	Application Implementation Consultant[DRA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB]	Privilege	CMR_MANAGE_COMPENSATION_PLAN_DEFINITION_PRIV	Manage Compensation Plan Definition	OPEN	SET	\$0461	1925	1	32081343	1257557943	1257569391	-
<input type="checkbox"/>	Manage Compensation and Manage Payroll Costing	Application Implementation Consultant[DRA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB]	Privilege	CMR_MANAGE_COMPENSATION_PLAN_DEFINITION_PRIV	Manage Compensation Plan Definition	OPEN	SET	\$0461	1925	1	32081343	1257557943	1257569391	-
<input type="checkbox"/>	Manage Employee Position and Manage Compensation	Application Implementation Consultant[DRA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB]	Privilege	CMR_MANAGE_COMPENSATION_PLAN_DEFINITION_PRIV	Manage Compensation Plan Definition	OPEN	SET	\$0461	1925	2	32081343	1257557943	1257569391	-
<input type="checkbox"/>	Manage Person and Manage Compensation	Application Implementation Consultant[DRA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB]	Privilege	CMR_MANAGE_COMPENSATION_PLAN_DEFINITION_PRIV	Manage Compensation Plan Definition	OPEN	SET	\$0461	1925	2	32081343	1257557943	1257569391	-
<input type="checkbox"/>	Manage Worker and Manage Compensation	Application Implementation Consultant[DRA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB]	Privilege	CMR_MANAGE_COMPENSATION_PLAN_DEFINITION_PRIV	Manage Compensation Plan Definition	OPEN	SET	\$0461	1925	2	32081343	1257557943	1257569391	-
<input type="checkbox"/>	Manage Compensation and Manage Payroll	Application Implementation Consultant[DRA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB]	Privilege	CMR_MANAGE_COMPENSATION_PLAN_DEFINITION_PRIV	Manage Compensation Plan Definition	OPEN	SET	\$0461	1925	1	32081343	1257557943	1257569391	-
<input type="checkbox"/>	Create User and Manage Compensation	Application Implementation Consultant[DRA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB]	Privilege	CMR_MANAGE_COMPENSATION_PLAN_DEFINITION_PRIV	Manage Compensation Plan Definition	OPEN	SET	\$0461	1925	2	32081343	1257557943	1257569391	-
<input type="checkbox"/>	Manage Worker and Manage Payroll Costing	Human Resource Specialist[DRA_PER_HUMAN_RESOURCE_SPECIALIST_JOB]	Privilege	PER_AUTO_CONVERT_PWSK_PRIV	Run Autoconvert Pending Workers Process	OPEN	SET	\$0461	1925	1	32564716	1257560143	1257565109	-

AccessPaaS \ Enterprise Access Monitor \ Analytics \ Violation Report \

Violations Summary Report

☒ Activity1 Name = 'NS-Vendor / Supplier Management'
 ☒ Activity2 Name = 'NS-Bill (Invoice) Payment'

User Name	Rule Name	Rule Type	Activity1 Name	Activity2 Name	Start Entry Name	Violation Entry	Violation Entry Name	Violation Entry Description	Violation Path Description	Violation Status	Exception Name	Exception Scope
1418	SoD - Vendor / Supplier Management and Bill (Invoice) Payment	SET	NS-Vendor / Supplier Management	NS-Bill (Invoice) Payment	NovaModule Shopify Integration Access	Permission	Pay Bills	Pay Bills	Role : NovaModule Shopify Integration Access->Permission : Pay Bills	OPEN	-	-
27	SoD - Vendor / Supplier Management and Bill (Invoice) Payment	SET	NS-Vendor / Supplier Management	NS-Bill (Invoice) Payment	KS Accountant (Reviewer)	Permission	Vendors	Vendors	Role : KS Accountant (Reviewer)->Permission : Vendors	OPEN	-	-
42444	SoD - Vendor / Supplier Management and Bill (Invoice) Payment	SET	NS-Vendor / Supplier Management	NS-Bill (Invoice) Payment	KS Accountant 3	Permission	Pay Bills	Pay Bills	Role : KS Accountant 3->Permission : Pay Bills	OPEN	-	-
758387	SoD - Vendor / Supplier Management and Bill (Invoice) Payment	SET	NS-Vendor / Supplier Management	NS-Bill (Invoice) Payment	KS Accountant 3	Permission	Pay Bills	Pay Bills	Role : KS Accountant 3->Permission : Pay Bills	OPEN	-	-
1208507	SoD - Vendor / Supplier Management and Bill (Invoice) Payment	SET	NS-Vendor / Supplier Management	NS-Bill (Invoice) Payment	Magento1 Novamodule Integration Access	Permission	Pay Bills	Pay Bills	Role : Magento1 Novamodule Integration Access->Permission : Pay Bills	OPEN	-	-

Automating Access Controls Analysis and Risk Remediation

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 permissions 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 most 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.

Provision Users with Policy Compliance

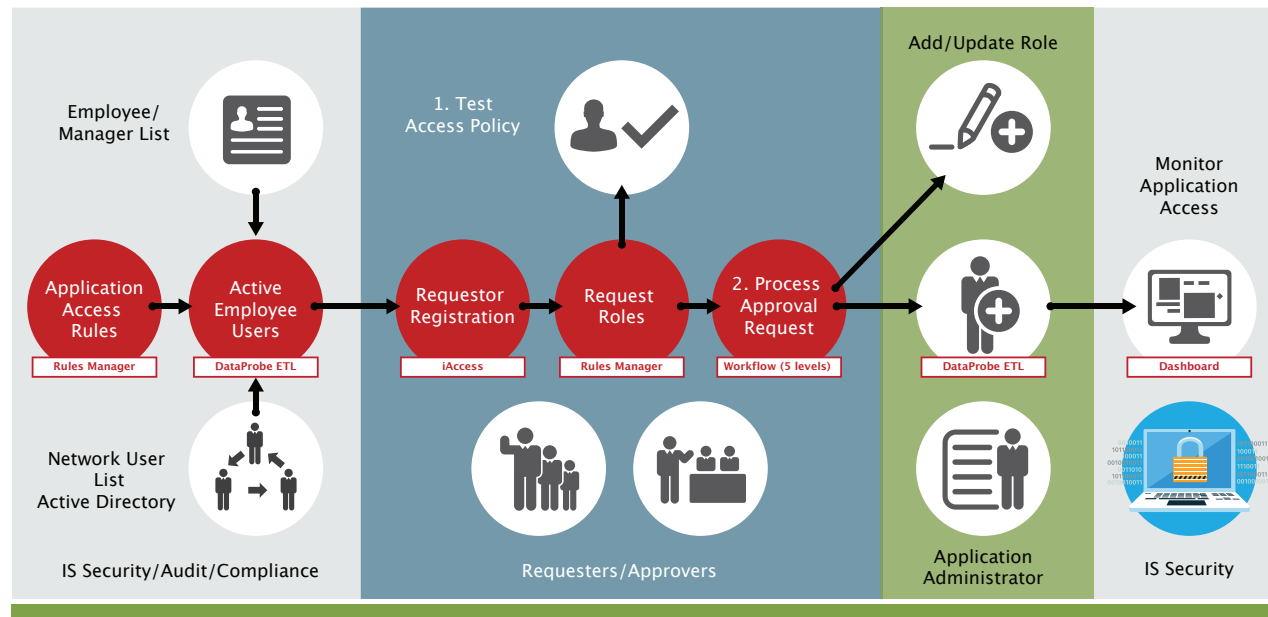
The user provisioning process provides an opportunity to prevent access violations through an automated workflow for review and approval process.

These include:

- Once user access violations in 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 to prevent repeating the remediation process during the next audit cycle.



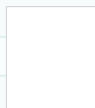



This swim-lane diagram shows the key activities by business roles that are required to support self-service user provisioning to ensure compliance with access policies:



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.

Manage Approval Hierarchy

Edit 	Approval level	Type	Approval role	Approval type	Active	Created by	Created date	Last updated by	Last updated date
	1	Primary	Manager	All	Y		12-JAN-22		12-JAN-22
	2	Primary	Role Group Primary Owner	Violations Only	Y		12-JAN-22		12-JAN-22
	3	Primary	Role Group Secondary Owner	Violations Only	Y		12-JAN-22		12-JAN-22

1 - 3

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 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 "privilege" manager familiar with the privileges in the requested Oracle Role. A technical manager with understanding of the Oracle security model may be assigned as a secondary approver.

User Requests for New Roles

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

This screen shot shows a user requesting Payables Vision Services R&D role:

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.

Select User

User Name

8024314

Go

Step 1 of 4 - User Information Review

Request New Access

User name	Active user	Employee name	Description	Manager name
8024314	Yes	Mohamed Nigab	Payables Manager	

1 rows selected

Total 1

Current Roles

Q

Go

Actions

Entry name	Entry type	Start date	End date	Request status
Employee(VIR_EMPLOYEE_ABSTRACT_DATA)	Role	01-JAN-70	-	Processed
Application Implementation Consultant(ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB)	Role	01-JAN-70	-	Processed
Audit Specialist - Global(VIR_AUDIT_SPECIALIST_GLOBAL_DATA)	Role	01-JAN-70	-	Processed
EAG ESS Monitor Role(VIR_EAG_ESS_MONITOR_ROLE)	Role	01-JAN-70	-	Processed
Project Team Member(ORA_PIF_PROJECT_TEAM_MEMBER_ABSTRACT)	Role	01-JAN-70	-	Processed
Digital Assistant - Employee Role(Digital_Assistant_Employee_Role)	Role	01-JAN-70	-	Processed
IT Security Manager(ORA_FND_IT_SECURITY_MANAGER_JOB)	Role	09-NOV-21	-	SOD Testing Done
IT Security Manager(ORA_FND_IT_SECURITY_MANAGER_JOB)	Role	09-NOV-21	-	SOD Testing Done
IT Security Manager(ORA_FND_IT_SECURITY_MANAGER_JOB)	Role	09-NOV-21	-	SOD Testing Done
IT Security Manager(ORA_FND_IT_SECURITY_MANAGER_JOB)	Role	09-NOV-21	-	SOD Testing Done

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 effect impacting multiple users with the change to a single role.

Select Access

Access Type: Accounts Receivable Manager[ORA_AR_ACCOUNTS_RECEIVABLE_MANAGER_JOB][ORA_AR_ACCOUNTS_RECEIVABLE_MANAGER_JOB] Go

Access Hierarchy Collapse All Expand All

Search

- Import Payables Invoice (Privilege)
- Manage Application Tree (Privilege)
- Manage Application Tree Label (Privilege)
- Manage Application Tree Structure (Privilege)
- Manage Orchestration Generic Web Service (Privilege)
- Manage Orchestration Order Billing Interface Web Service (Privilege)
- Manage Orchestration Order Modification (Privilege)
- Manage Receivables Activities (Privilege)
- Manage Receivables Balances Activities (Privilege)
- Manage Receivables Business Intelligence (Privilege)
- Manage Trading Community Hierarchy (Privilege)
- Manage Unpaid Receivables Bill Receivable (Privilege)
- Override Receivables Receipt Application (Privilege)
- Run Actual Receipts Report (Privilege)
- Run Adjustments Journal (Privilege)
- Run Adjustments Register (Privilege)
- Run Applied Receipts Journal (Privilege)
- Run Applied Receipts Register (Privilege)
- Run Bad Debts Provision Report (Privilege)
- Run Cross Currency Exchange Gain and Loss Report (Privilege)

Access Hierarchy (Inherited)

Go Actions

Navigation Path	Privilege	Hierarchy Id
<< RoleAccounts Receivable Manager[ORA_AR_ACCOUNTS_RECEIVABLE_MANAGER_JOB] << RoleAccounts Receivable Monitoring[ORA_AR_ACCOUNTS_RECEIVABLE_MONITORING_DUTY]	PrivilegeGenerate Automatic Receipt Write-offs	174031959
<< RoleAccounts Receivable Manager[ORA_AR_ACCOUNTS_RECEIVABLE_MANAGER_JOB] << RoleAccounts Receivable Monitoring[ORA_AR_ACCOUNTS_RECEIVABLE_MONITORING_DUTY]	PrivilegeGenerate Customer Statements	174031959
<< RoleAccounts Receivable Manager[ORA_AR_ACCOUNTS_RECEIVABLE_MANAGER_JOB] << RoleAccounts Receivable Monitoring[ORA_AR_ACCOUNTS_RECEIVABLE_MONITORING_DUTY]	PrivilegeManage Receivables Balances Activities	174031959
<< RoleAccounts Receivable Manager[ORA_AR_ACCOUNTS_RECEIVABLE_MANAGER_JOB] << RoleAccounts Receivable Monitoring[ORA_AR_ACCOUNTS_RECEIVABLE_MONITORING_DUTY]	PrivilegeManage Receivables Late Charge Batch	174031959
<< RoleAccounts Receivable Manager[ORA_AR_ACCOUNTS_RECEIVABLE_MANAGER_JOB] << RoleAccounts Receivable Monitoring[ORA_AR_ACCOUNTS_RECEIVABLE_MONITORING_DUTY]	PrivilegeReview Customer Account Activities	174031959
<< RoleAccounts Receivable Manager[ORA_AR_ACCOUNTS_RECEIVABLE_MANAGER_JOB] << RoleAccounts Receivable Monitoring[ORA_AR_ACCOUNTS_RECEIVABLE_MONITORING_DUTY]	PrivilegeRun Account Status Report	174031959
<< RoleAccounts Receivable Manager[ORA_AR_ACCOUNTS_RECEIVABLE_MANAGER_JOB] << RoleAccounts Receivable Monitoring[ORA_AR_ACCOUNTS_RECEIVABLE_MONITORING_DUTY]	PrivilegeRun Billing History Report	174031959

AccessPaaS \ Enterprise Access Monitor \ Define Scope \ Manage Rules \

Rule Details

Environment CloudERP_Internal

Name Create Payables Invoices and Create Payments

Approval Status New

Show All Rules Rule Attributes Activities Exceptions People History

Rules Cancel Edit R

Description Can cause payments and cash to be inappropriately processed and therefore affecting a company's assets.

Rule Attributes

Risk Level HIGH


Rule Type Incompatible Sets

Rule Objective SOD Detective

Start Date 01-JUL-21

End Date

21 | www.safepaas.com

 SafePaaS™

© SafePaaS 2022

Activities

Set1 Activity Create Payments

Set2 Activity Create Payables Invoices

Entry Name	User Entry Name	Entry Type	Activity Set ↑	Last Updated By	Last Updated Date
AP_CREATE_PAYABLES_PAYMENT_PRIV	Create Payables Payment	Privilege	Set1 Activity	FITADMIN	05-JUL-21
AP_EDIT_PAYABLES_PAYMENT_PRIV	Edit Payables Payment	Privilege	Set1 Activity	FITADMIN	05-JUL-21
AP_MANAGE_PAYABLES_PAYMENTS_PRIV	Manage Payables Payments	Privilege	Set1 Activity	FITADMIN	05-JUL-21
AP_MANAGE_PAYABLES_PAYMENT_PROCESS_REQUEST_PRIV	Manage Payables Payment Process Request	Privilege	Set1 Activity	FITADMIN	05-JUL-21
AP_MANAGE_PAYABLES_PAYMENT_PROCESS_REQUEST_TEMPLATE_PRIV	Manage Payables Payment Process Request Template	Privilege	Set1 Activity	FITADMIN	05-JUL-21
AP_PROCESS_PAYABLES_PAYMENT_PROCESS_REQUEST_PRIV	Process Payables Payment Process Request	Privilege	Set1 Activity	FITADMIN	05-JUL-21
AP_REISSUE_PAYABLES_PAYMENT_PRIV	Reissue Payables Payment	Privilege	Set1 Activity	FITADMIN	05-JUL-21
AP_STOP_PAYABLES_PAYMENT_PRIV	Stop Payables Payment	Privilege	Set1 Activity	FITADMIN	05-JUL-21
AP_SUBMIT_PAYABLES_PAYMENT_PROCESS_REQUEST_PRIV	Submit Payables Payment Process Request	Privilege	Set1 Activity	FITADMIN	05-JUL-21
AP_CREATE_PAYABLES_INVOICE_PRIV	Create Payables Invoice	Privilege	Set2 Activity	FITADMIN	05-JUL-21

1 - 10

This screenshot shows a new target role “Create Payables Invoices and Create Payments”

This role has a number of SoD access policy violations including “Create Supplier” and Create Payments.”

Violations by User Report in SafePaaS

These violations identify users who can create ERP users /employees and update their compensation. Someone could create a person as a user who is not an employee, but also create a compensation package for this user; in an attempt to create fraud.

AccessPaaS \ Enterprise Access Monitor \ Analytics \ Violation Report \

Violations by User Report

Environment:

Test Name:

User Violation Report Export All Violations

User Name	Rule Name	Rule Type	Activity Name	Violation Path Description	Violation Status	Exception Name	Exception Scope
Arul.Das@no_email.com : Arul.Das@no_email.com	6921: Enter Journals and Set Up General Ledgers	SET	Enter Journals	Role : General Accounting Manager->Privilege : Manage Journal Requiring Approval	OPEN	-	-
Tony.Lee@no_email.com : Tony.Lee@no_email.com	6921: Enter Journals and Set Up General Ledgers	SET	Enter Journals	Role : General Accounting Manager->Privilege : Manage Journal Requiring Approval	OPEN	-	-
Bhaskar.swamy@no_email.com : Bhaskar.swamy@no_email.com	6921: Enter Journals and Set Up General Ledgers	SET	Enter Journals	Role : General Accounting Manager->Privilege : Manage Journal Requiring Approval	OPEN	-	-
John.Shaun@no_email.com : John.Shaun@no_email.com	7554: Post Journal Entry and Set Up General Ledgers	SET	Post Journal Entry	Role : Cost Accountant->Privilege : Post Journal	OPEN	-	-
Johnson.Nick@no_email.com : Johnson.Nick@no_email.com	7552: Post Journal Entry and Define Accounting Calendars	SET	Post Journal Entry	Role : Cost Accountant->Privilege : Post Journal	OPEN	-	-
Joseph.Hilton@no_email.com : Joseph.Hilton@no_email.com	7552: Post Journal Entry and Define Accounting Calendars	SET	Post Journal Entry	Role : Cost Accountant->Privilege : Post Journal	OPEN	-	-
John.Shaun@no_email.com : John.Shaun@no_email.com	7552: Post Journal Entry and Define Accounting Calendars	SET	Post Journal Entry	Role : Cost Accountant->Privilege : Post Journal	OPEN	-	-

Here you can remediate the violations:

AccessPaaS \ Enterprise Access Monitor \ Detect Violations \

Manage Violation

Test Name

* Environment: * Request Name:

Manage Violation Submit Export All Violations

Exception Type:

Exception Scope:

Select All

UnSelect All

Select	Rule Name	Start Entry Name	Violation Entry	Violation Entry Name	Violation Entry Description	Violation Status	Rule Type	Company id	Group id	Rule activity group	User id	Start entry id	Child entry id	Hierarchy path id
<input checked="" type="checkbox"/>	6921: Enter Journals and Set Up General Ledgers	General Accounting Manager	Privilege	GL_APPROVE_JOURNAL_PRIV	Manage Journal Requiring Approval	OPEN	SET	3542	360	1	21995464	1255678773	1255681891	-
<input checked="" type="checkbox"/>	6921: Enter Journals and Set Up General	General Accounting Manager	Privilege	GL_APPROVE_JOURNAL_PRIV	Manage Journal Requiring Approval	OPEN	SET	3542	360	1	21995318	1255678773	1255681891	-

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 ensures more effective audit of compliance with the organization's access policies.

This is an example of the display screen that provides real time status to all self-service user-provisioning requests:

Network id	Email	Request status	Requested date	Requested by	Role key	Role name	Approval type	Approval role	Active	Approver	Approver name	Approval status
8034554	[REDACTED]	SOD Test Done	18-OCT-21	MEKANAYAKE	ORA_GL_GENERAL_ACCOUNTANT_JOB	General Accountant(ORA_GL_GENERAL_ACCOUNTANT_JOB)	Primary	Manager	Y	S003304		Rejected
8034554	[REDACTED]	SOD Test Done	18-OCT-21	MEKANAYAKE	ORA_GL_GENERAL_ACCOUNTANT_JOB	General Accountant(ORA_GL_GENERAL_ACCOUNTANT_JOB)	Primary	Role Group Secondary Owner	Y	SASUKE	SASUKE	Pending
8034554	[REDACTED]	SOD Test Done	18-OCT-21	MEKANAYAKE	ORA_GL_GENERAL_ACCOUNTANT_JOB	General Accountant(ORA_GL_GENERAL_ACCOUNTANT_JOB)	Primary	Role Group Primary Owner	Y	NARUTO	NARUTO	Pending

1 - 3

- In this workflow approvers receive notifications to approve or reject each user access request. The request includes the roles 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 SafePaaS using standard security APIs to provision user and role 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.

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 role 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 privileges.
- 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 be considered as part of your compensating control strategy to manage overall access risks.

Emma Kelly
Marketing Manager

Emma.kelly@safepaas.com
www.safepaas.com