ORACLE

Optimize Security Design and Provisioning

Step-by-step guide to optimizing Fusion Cloud ERP roles and their provisioning

December 2020 | Version 2

SUMMARY

Whether your organization is just getting started with a Cloud ERP implementation or already live, now is the best time to ensure that security is enforced in your role design, configuration and provisioning processes. You can ensure that roles are free of separation of duties (SoD) conflicts, find users who will be granted sensitive access, and automate the assignment of roles to users in order to minimize SoD conflicts arising from combinations of roles.

This document gives step-by-step instructions to:

1. Automate security & SoD analysis
   - Employ Oracle's *Secure By Design* methodology (see below)
   - Show SoD risk exposure in minutes
   - Activate 12 critical SoD rules (for payables, purchasing, general ledger, and receivables)
   - Streamline security analysis required while building custom Job Roles
   - Identify non-compliant test users and the risks they pose
   - Provide guidance for SoD conflict remediation
   - Reduce security design effort and minimize rework costs

2. Enforce SoD & restricted access rules
   - Ensure that ERP auto-provisioning role mappings are compliant
   - Validate that user provisioning via IDM tools is compliant

Oracle's *Secure By Design* methodology for Fusion Cloud ERP

1. Document, review and prioritize ERP user access rules
   - Build a risk-prioritized list of SoD and restricted access policies
   - Review and assess those policies every six months, and when there are events that have material impact on risk (for example, deployment of a new ERP module, merger/acquisition, significant growth)

2. Evaluate the security impact of your ERP configuration choices
   - Enforce the *standard of least-privilege* for each role to minimize risk exposure downstream while enabling employees to complete their tasks
   - Document reasons for accepting risks; this accelerates identification and resolution of unexpected security findings

3. Use *responsibility-based access* approach to prevent security issues
   - ERP tasks are initiated and completed based on the employee's primary responsibilities within your organization
   - Map, review and enforce this predictable access via functional and data security permissions

4. Build data-driven continuous feedback loops that ensure ongoing enforcement of security rules
    - Review changes to user access to identify SoD and restricted-use violations
    - Conduct periodic audits of critical ERP configuration and transaction data to ensure access security rules are enforced consistently

5. Promote accountability – and place exception approval authority – with business process owners
    - Enable process owners to review and approve each security exception. (Process owners are the domain experts in payables, receivables, general ledgers, etc., and therefore best equipped to assess business risk associated with security rules and violations.)
    - Periodically certify each ERP user who has access to sensitive functions and data (to ensure top-down validation).

The methodology's objectives are to:

- Enable "baked-in" tactics needed to manage ERP authorization & security models, even when they are complex, recursive and/or dynamic.

- Achieve the risk-based audit-ready separation of duties (SoD) and restricted/sensitive access (RSA) programs required for Sarbanes Oxley and similar statutory or regulatory initiatives.

- Promote a security-aware culture that protects business data from insider threats, financial fraud, theft, misuse and human error.

Oracle Risk Management is integral to the methodology:

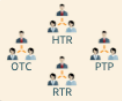
1. Provides the foundation needed to automate accurate ERP security analysis
    - Graph-based analytic engine that supports fine grain analysis of complex, hierarchical and recursive security structures.
    - Accurately and reliably review and visualize the entire path by which any user is able to access and execute sensitive functions.
    - Pre-integrated, real-time feed from the authoritative security store (Fusion Security Store).

2. Automates use cases in each phase of the ERP lifecycle: design, configure, test, go-live and sustain use
    - Leverage an audit-approved library of ERP security rules.
    - Apply the same rules from Day 1 in your ERP deployment journey.
    - Automate the analysis required to configure compliant, least-privilege roles.

3. Promotes risk awareness through transparency, actionable analysis, and simple workflows for key stakeholders in audit, IT, and lines of business
    - Continuous monitoring of user access and activity to identify security violations.
    - Unified risk dashboard and incident workflows for business process owners, internal auditors, and IT security managers.
    - Periodic and event-based continuous certification of employee access to sensitive ERP functions that can reviewed by the employee's manager.

Stakeholder Engagement

Several kinds of people are likely to be involved in this activity:

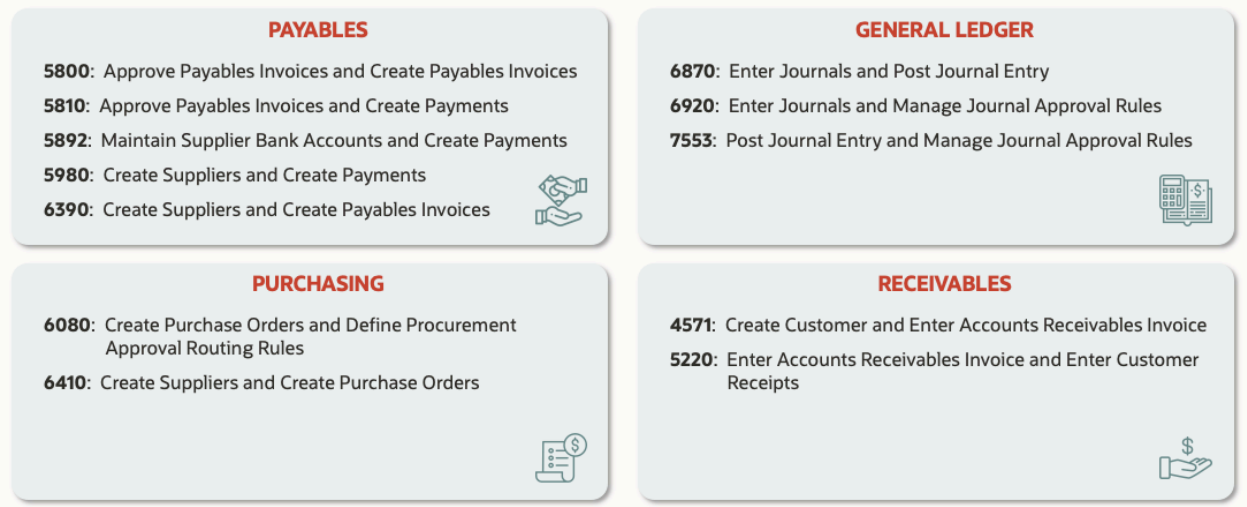
	Role	Activity	Value/Benefit
	**Audit/Compliance Team** *Internal Audit, Financial Governance & Compliance*	*Define, prioritize and deploy SoD and restricted access rules*	*Achieve compliance from day 1 and automate SoD reports for external and internal audit*
	**Fusion Implementers** *IT Organization, Financial & HR Systems, IT Consultants*	*Build compliant custom roles and provision employees prior to go-live*	*Automate security analysis required while configuring new roles and provisioning workflows*
	**Business Process Owners** *Controller, AP, GL, AR, Expenses, Procurement Manager*	*Identify employees and access based on org and position*	*Meet SoD/access control requirements and streamline exception management*
	**IT Security Team** *ERP/HCM Security Manager, IT Security Admin*	*Maintain compliant custom roles and provision new employees after go-live*	*Automate security & SoD analysis required while modifying existing roles and adding new users*

OUTCOMES & BENEFITS

The step-by-step configuration instructions in this blueprint can be completed in days (approximately one week) and offers the following benefits and outcomes:

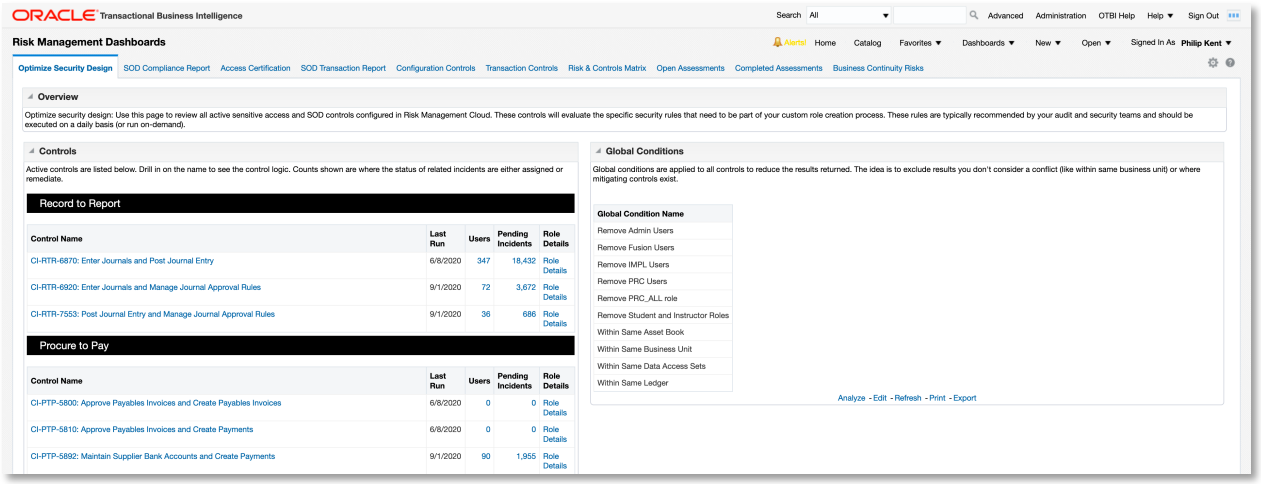
Activate Key Separation of Duties (SoD) Rules

This blueprint includes instructions for 12 key rules typically required by most auditors. They have been selected from a library of 100+ pre-built rules.

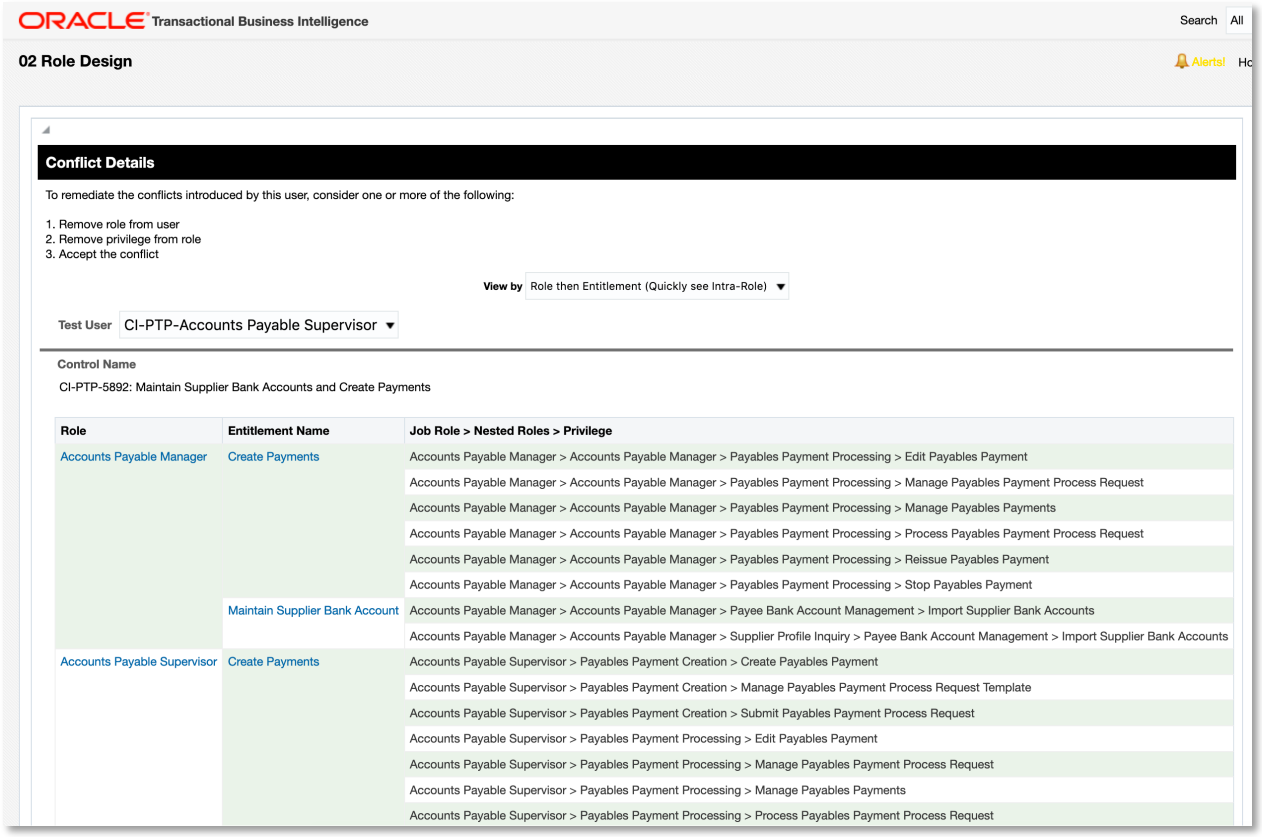


Eliminate SOD risk within a single Fusion Job Role

Remove intra-role violations

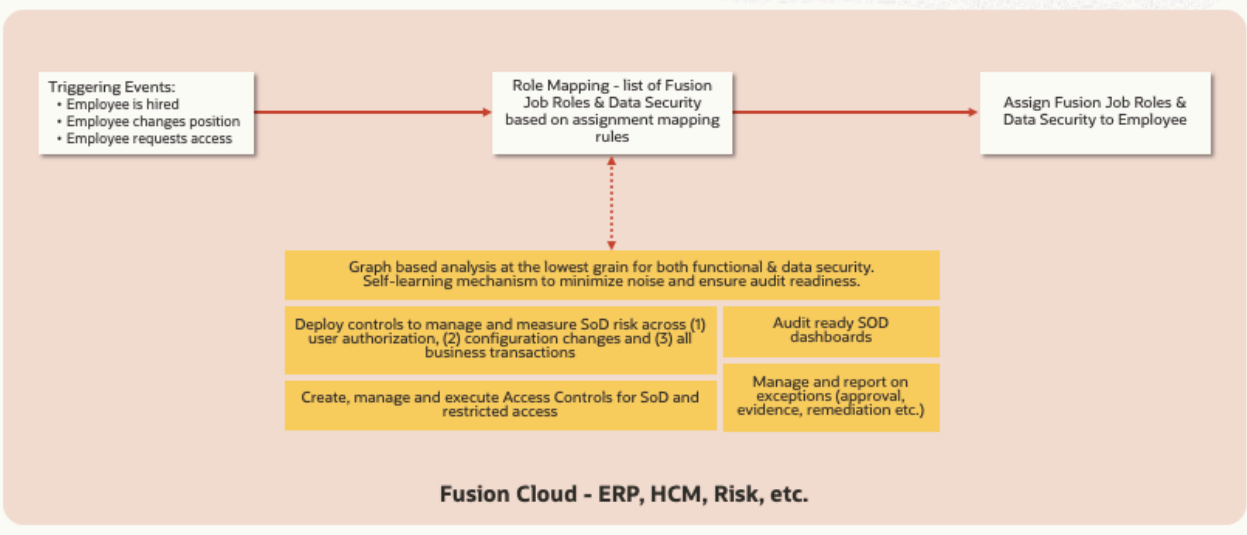


Evaluate detailed results needed to fix high-risk Roles

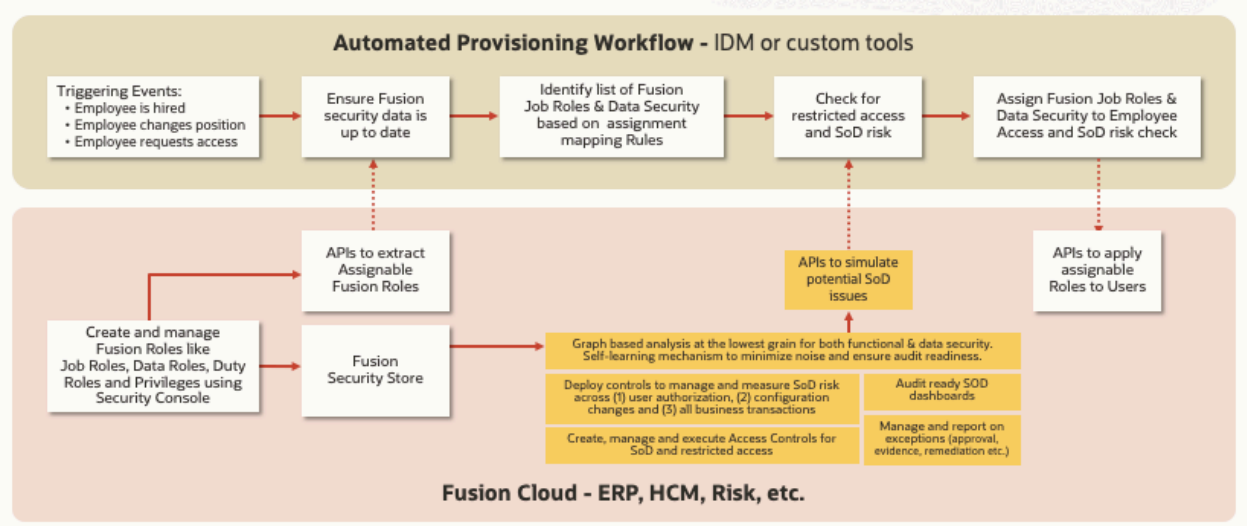


Enable role provisioning automation that benefits from deep SoD analysis

If deploying Fusion-based auto-provisioning role mappings – whether stand-alone, in conjunction with HCM Hire / Data Loader, or in conjunction with external IDM user provisioning that assigns user attributes (e.g., position, department, etc.) – use SoD analyses to achieve compliant mappings:



If deploying external IDM user provisioning that assigns Fusion roles (less desirable than the approach above because it fragments role management between Fusion and the IDM), use Risk Management APIs to provide SoD analyses before assigning the Fusion roles to users:



GET STARTED

If you've implemented another Risk Management blueprint in the past, you may find that some or all of these steps have already been done. If so, fantastic – move on to the next step or section!

Configurations

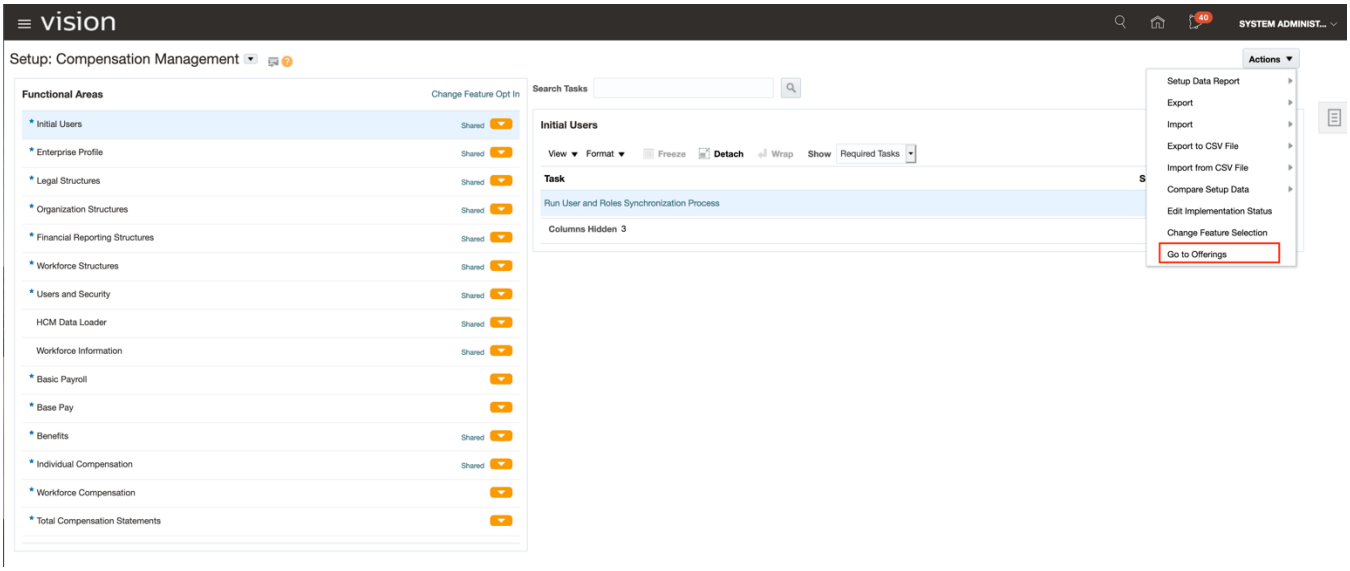
Overview & Participants

Your security team will enable the Risk Management offering and grant access to the business process owners and the risk & compliance team.

Your risk & compliance team will deploy and maintain controls, schedule jobs and deploy your Risk Management dashboard.

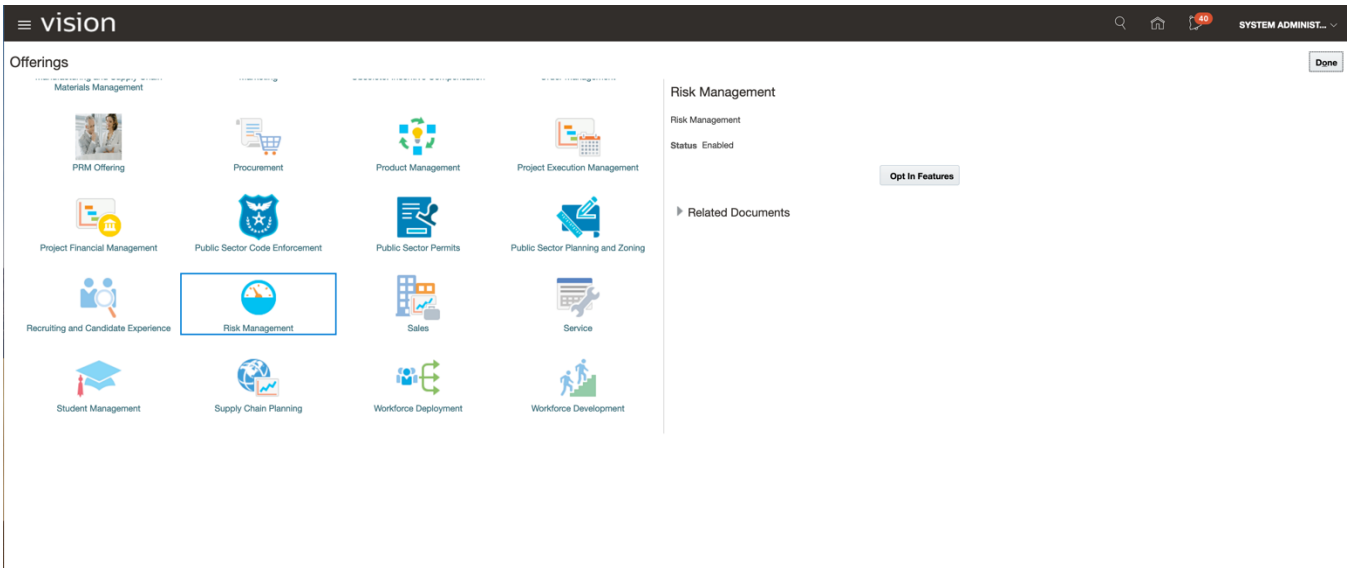
Step 1: Activate Risk Management

Your first step is to make sure Risk Management is activated in your environments. Ask your system administrator to navigate to Setup and Maintenance:



Then, navigate to Actions > Go to Offerings.

On the Offerings page, click on ‘Risk Management’ and make sure Status is ‘Enabled’:



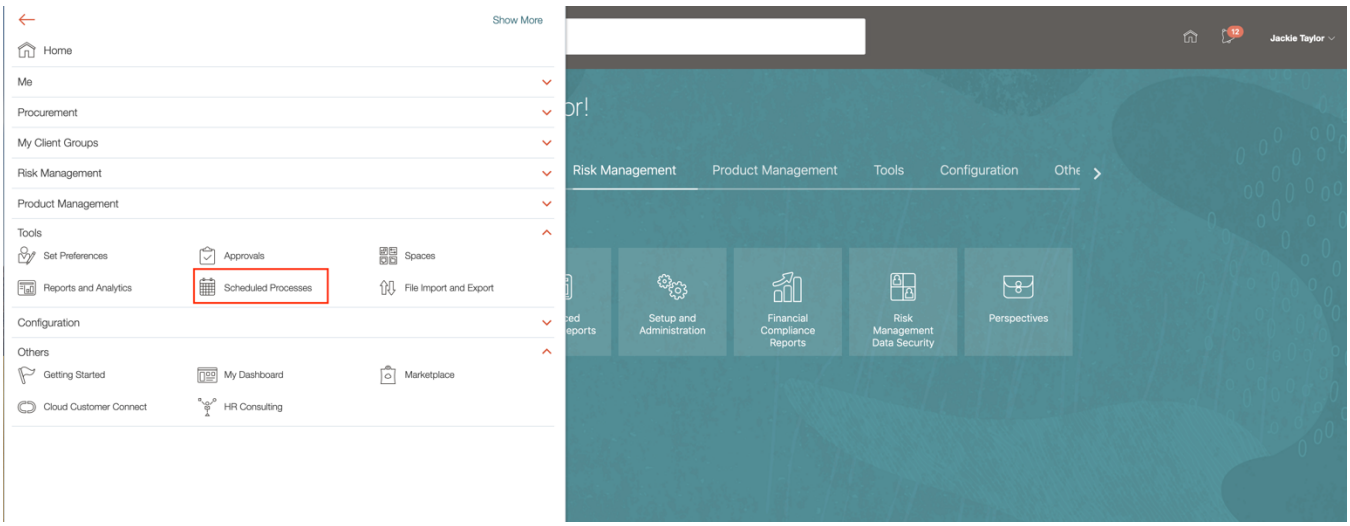
Step 2: Assign Risk Management Job Roles

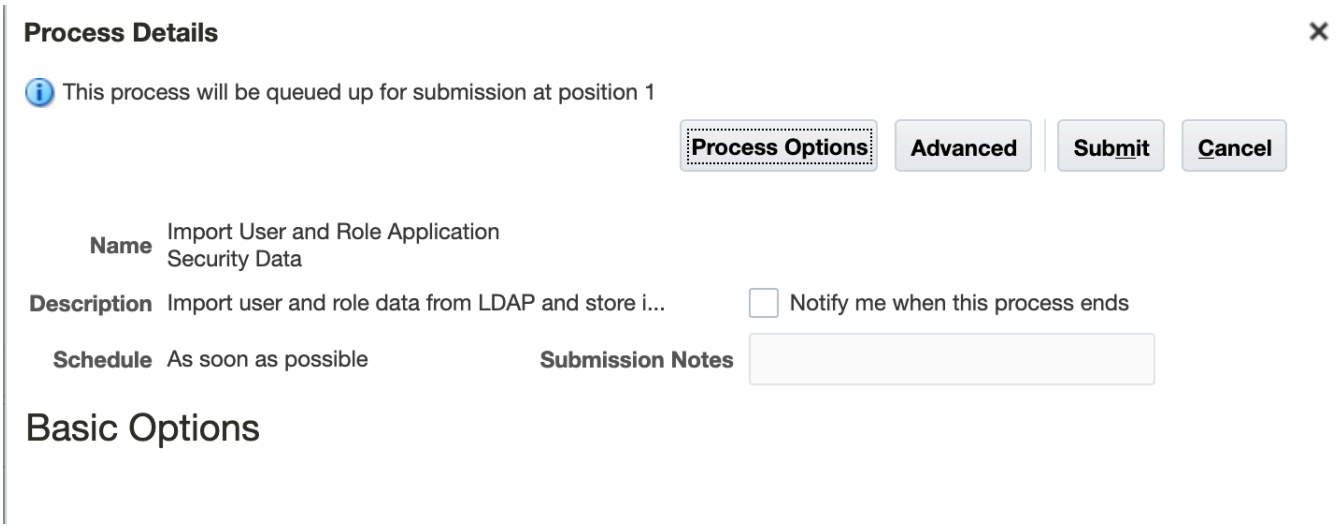
Assign your compliance team members the following job roles:

1. Risk Administrator
2. Advanced Access Controls Analyst

Step 3: Run the Import User and Role Application Security Data Process

Most likely this is already a scheduled job that runs several times each day. However, that may not be the case in a development environment. To make sure, navigate to Scheduled Processes and run the “Import User and Role Application Security Data” process. You might need someone with IT Security Manager access to help you.

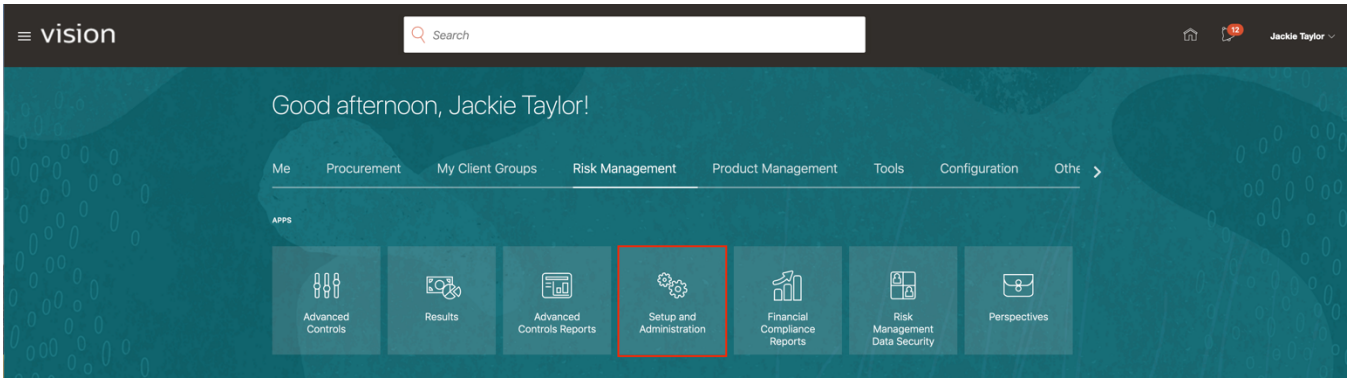


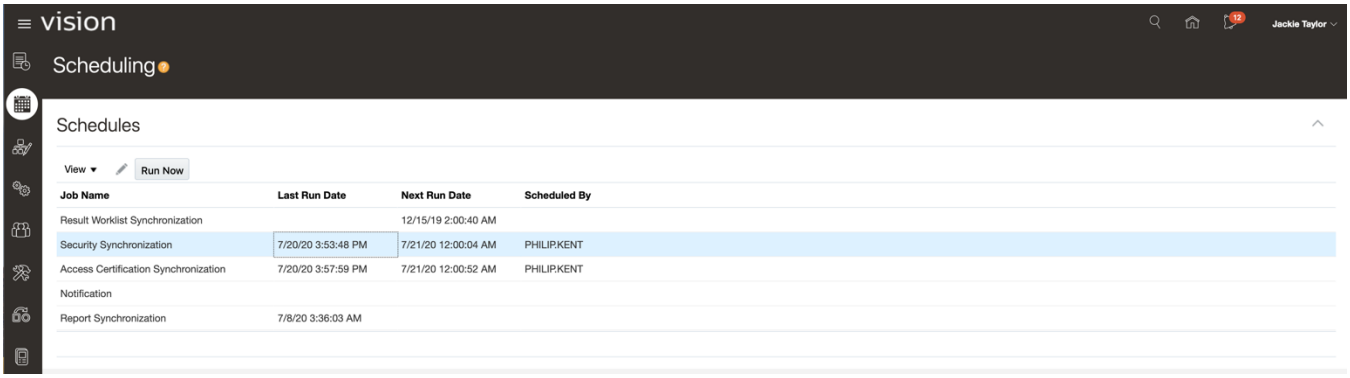


Step 4: Run the Security Synchronization Job

Anytime you make changes in Security Console, be sure to follow up by running the Security Synchronization job, which updates who can access what in Risk Management. The job should be scheduled to run at least daily.

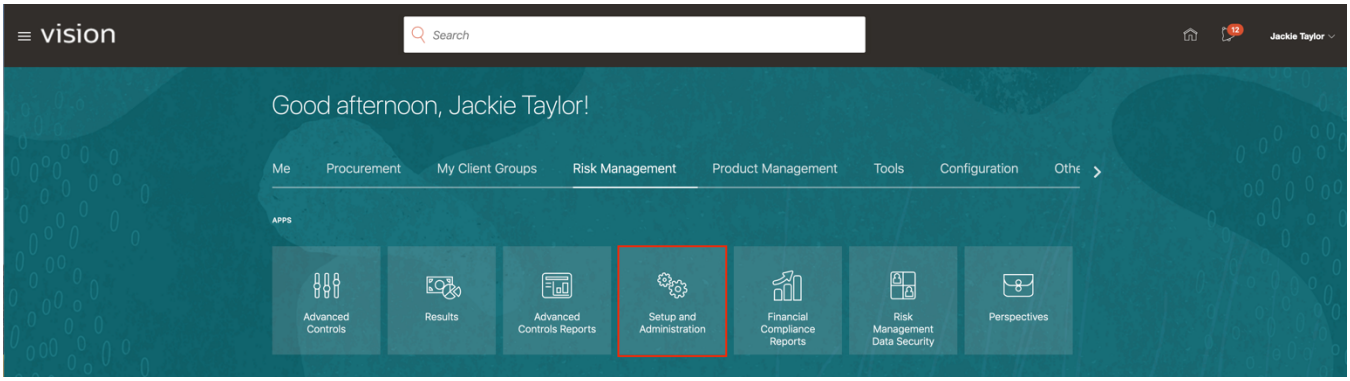
Navigate to Risk Management > Setup and Administration, then click the Scheduling tab:



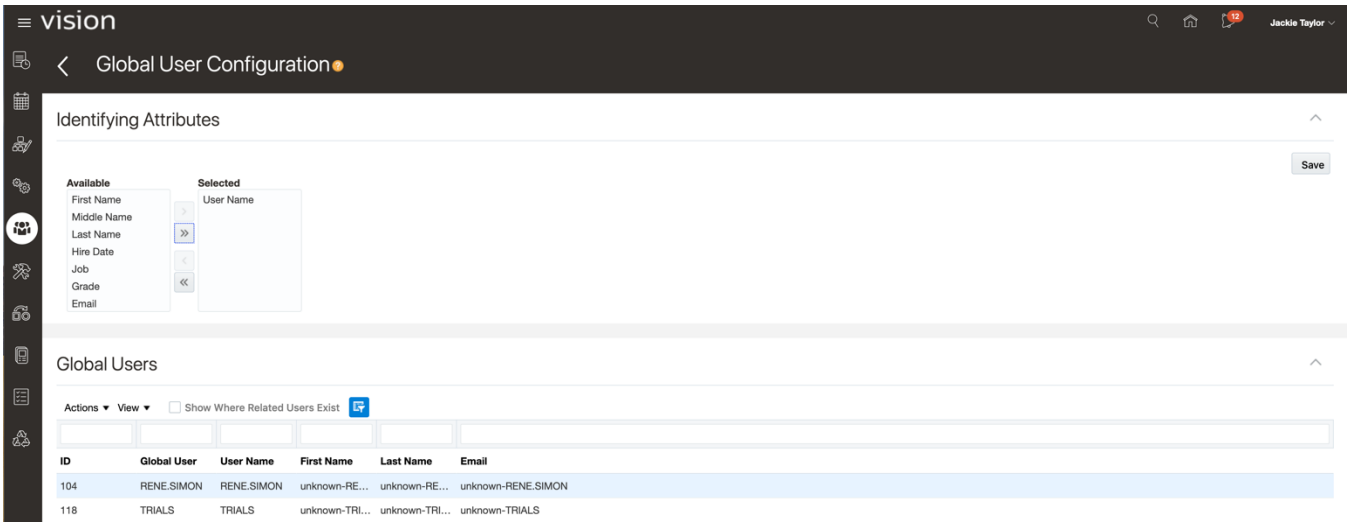


Step 5: Configure Global Users and Run the Global User Synchronization Job

Navigate to Risk Management and click Setup and Administration:



Select the tab that has a group of people on it. Then select the identifying attribute(s); you'll want to select an attribute that is unique – for example, user name. Next select Actions > Run from the Global Users section:

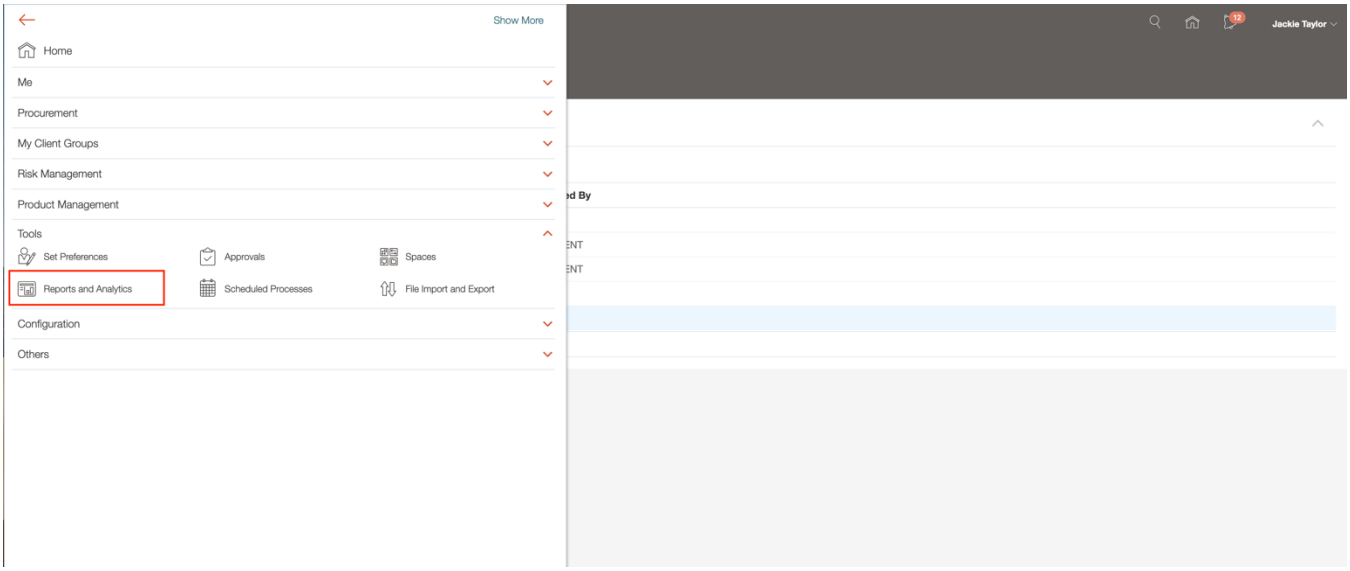


Once that job completes, the Global Users section is populated. These are users synchronized from the Users area in Security Console. The job role assignments for these users will be evaluated during control analysis, and the global user name is the value associated to incidents identified.

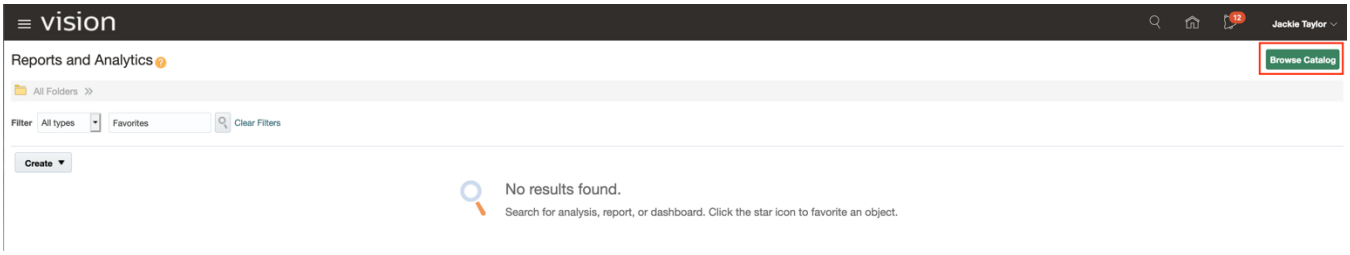
Step 6: Deploy the Risk Management Dashboard

To deploy the Risk Management Dashboard, you must have a job role that grants access to the BI Administrator duty role. Ask a system administrator to help you; there might already be a job role with the access needed.

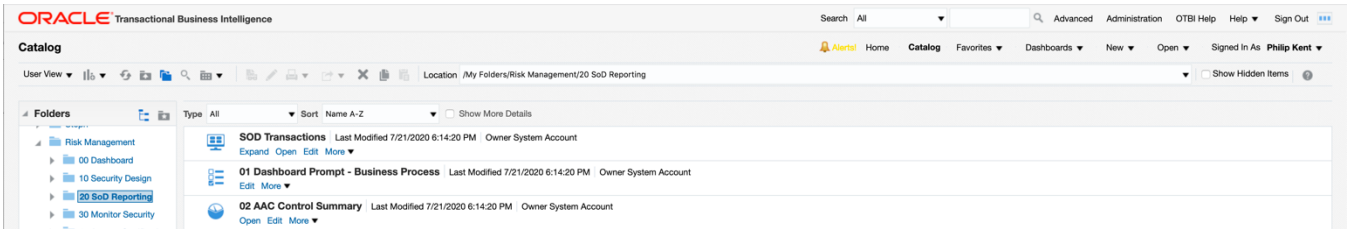
Navigate to Reports and Analytics, then select Browse Catalog:



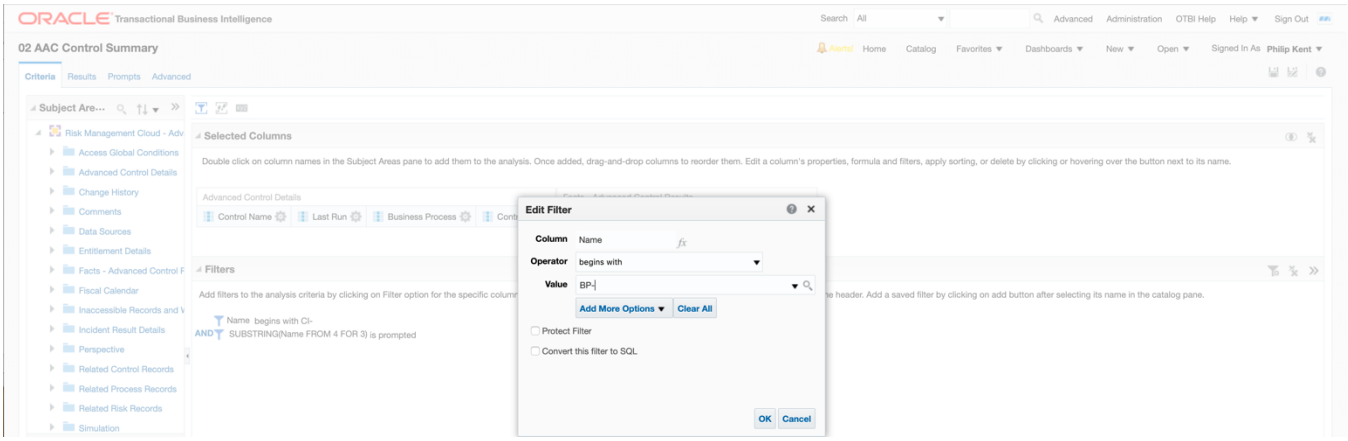
Under Shared Folders, select Custom. Unarchive our Solution Blueprint Risk Management catalog: https://cloudcustomerconnect.oracle.com/posts/6ac0498b5e; that will create a Risk Management folder. Select "00 Dashboard," then click edit on the Risk Management Dashboards:



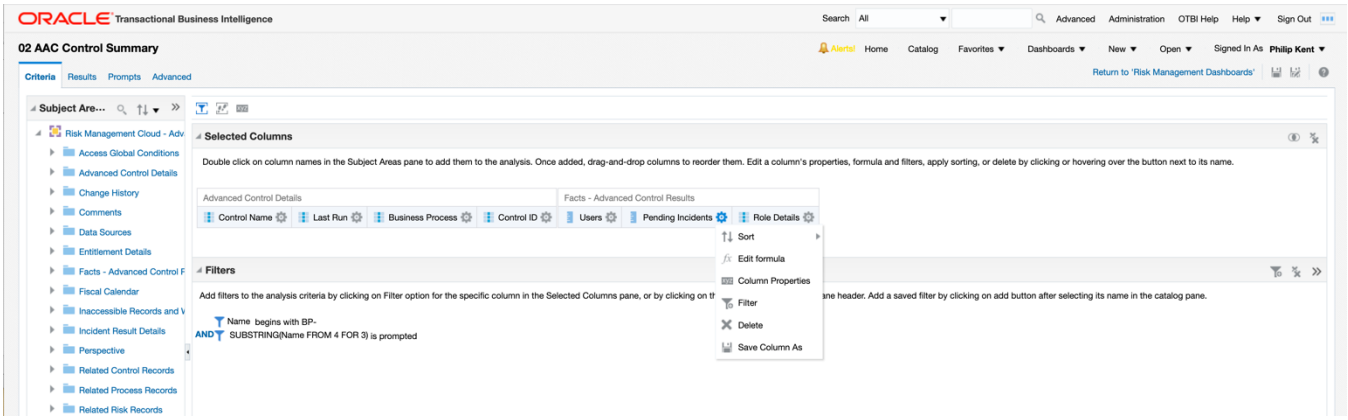
Edit the "02 AAC Control Summary" analysis found in the "Risk Management > 20 SoD Reporting" folder:



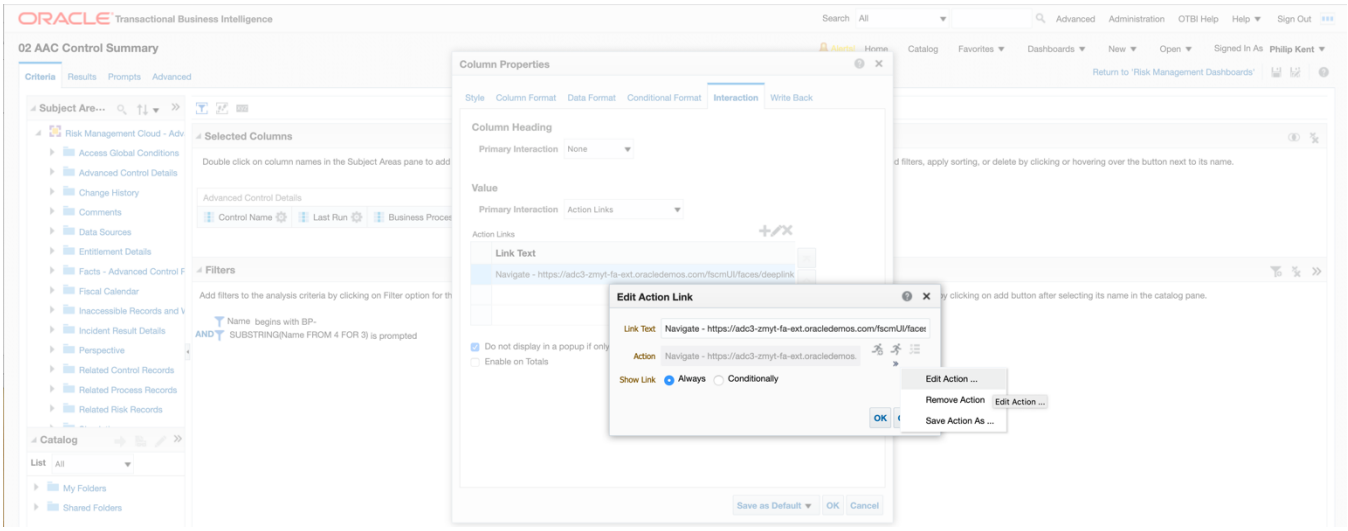
Click the Criteria tab and edit the “Name begins with CI-“ filter and change this to “BP-“ (or however you prefer to prefix your controls):



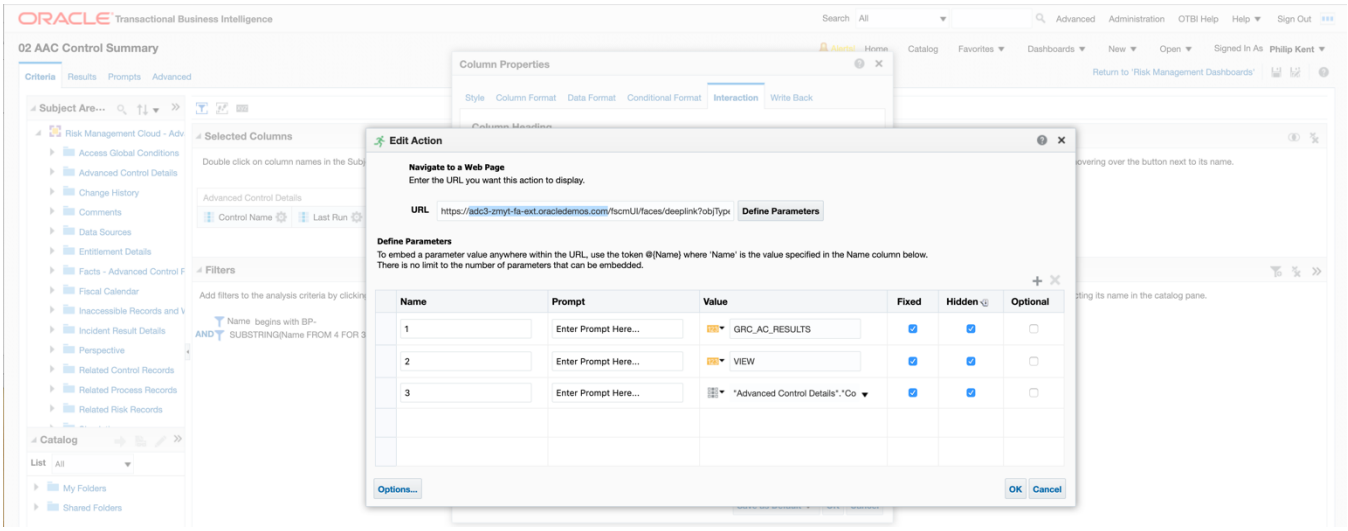
Click OK in the Edit filter pop up. Then click the gear box on the Pending Incidents column and select column properties:



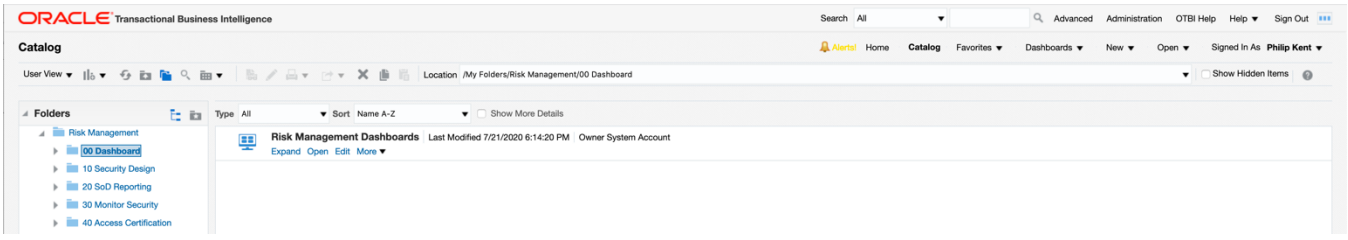
Edit the action link URL:



Replace the host name (highlighted below) with the host name of your environment:



Save the report and run the dashboard by navigating to the “00 Dashboard” and click on Open for the “Risk Management Dashboards”:



Create User Assignment Security Groups

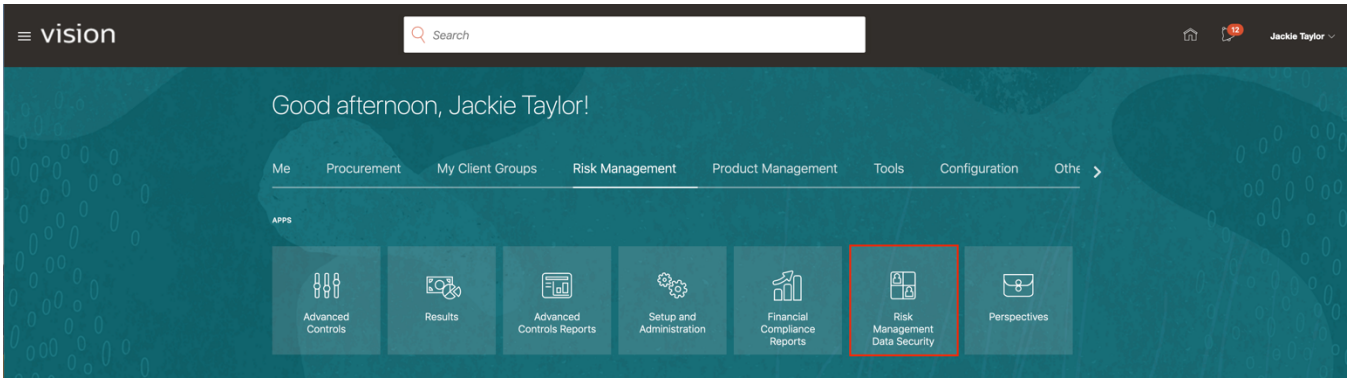
The most scalable approach to setting up security in Risk Management is to create a user assignment group, even if only one person is in that group. Later, if you need to add or change a group's members, it's easy.

Overview & Participants

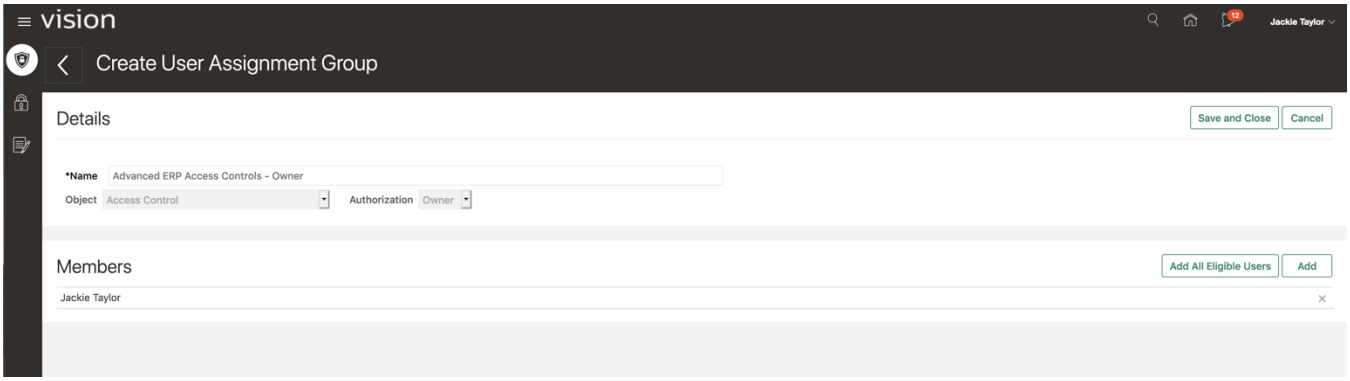
The Risk & Compliance team will create user assignment security groups and assign appropriate authorizations to models, controls and results.

Step 1: Create User Assignment Group for Controls

Navigate to Risk Management > Risk Management Data Security:



Click Add to open a new page, then enter the details of the user assignment group. In the below example, a new group with the name “Advanced ERP Access Controls – Owner” is created with Object set to “Access Control” and Authorization set to “Owner”:

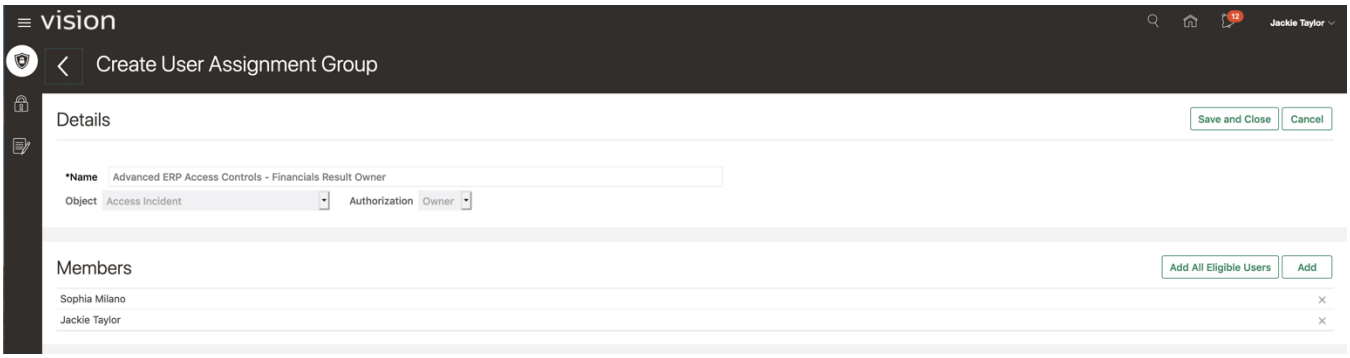


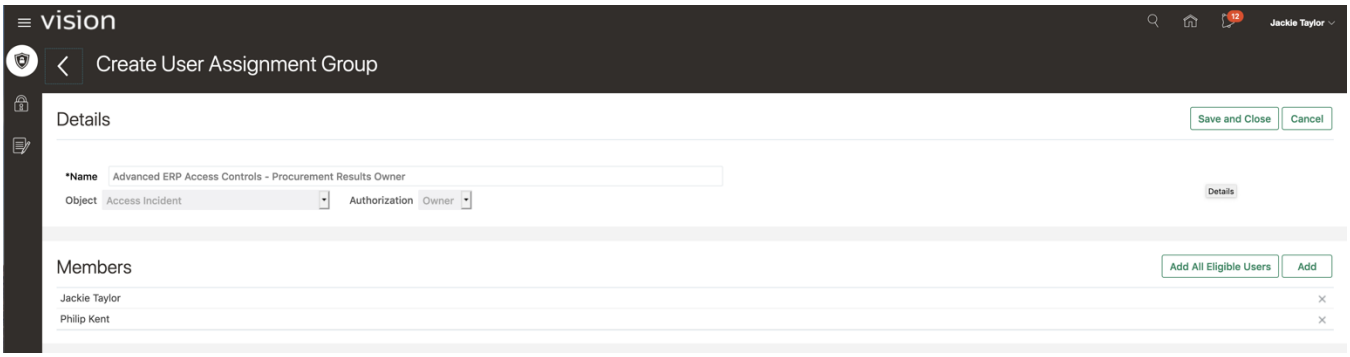
In the Members section, click Add and select one or more members. These are people who will be able to view, edit and assign security to access control records. For now, this is sufficient. As your project evolves, you may decide to add additional user assignment groups where members are only authorized to view records for example.

Step 2: Create User Assignment Group for Control Results

Navigate to Risk Management > Risk Management Data Security.

For each control, you can set the default security assigned to generated results. Follow the same process as above, but this time select the “Access Incidents” object. In this example, we’ll create two different groups: one will investigate test user results generated by financial controls, and the other will investigate test user results generated by procurement controls:




vision
Jackie Taylor
Create User Assignment Group
Details
Save and Close
Cancel
*Name
Advanced ERP Access Controls - Procurement Results Owner
Object
Access Incident
Authorization
Owner
Details
Members
Add All Eligible Users
Add
Jackie Taylor
Philip Kent

PART 1 – AUTOMATING SECURITY ANALYSIS WHEN BUILDING ROLES

Often the process of structuring roles and determining if the combination of roles granted to a user will cause conflicts involves comparing privileges that make up the roles granted to a user with privileges that are in conflict. This is often a manual effort extracting data and cross referencing in spreadsheets and documents, etc. This section will step you through a process using Risk Management that will help to automate security analysis with test users.

Create Test Users & Assign Roles

Overview & Participants

The ERP implementation consultants work with the business process owners to define various job role positions, such as a general accountant and the types of functional access a general accountant would need to do their job.

Your security team will create test users, custom job roles and assign those roles to the test users. Ultimately, the security team will also create role mappings to automate role provisioning to users.

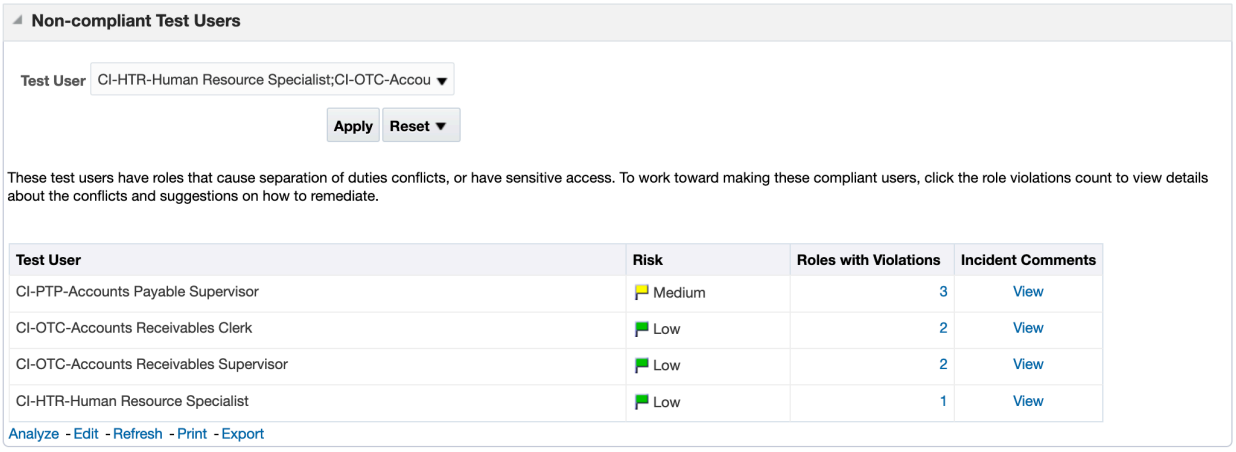
Step 1: Identify and Create Test Users

The idea of a test user is to create a persona that will be used to test out functional access. For example, in a company there may be general accountants, accounts payables supervisors, accounts payables clerks, accounts receivables supervisors, purchasing agents and so on. If the company has an average of 5 accounts payables clerks, and every time an AP clerk is hired the same set of roles should be granted, then it makes sense to automate that process.

So, create the test user personas that fit your business. Follow a naming convention that will help during the security design process. For example, you may create the following test users:

User Name
CI-HCM-Human Resource Specialist
CI-PTP-Accounts Payable Supervisor
CI-PTP-Accounts Payable Clerk
CI-PTP-Procurement Agent Buyer
CI-RTR-General Accountant
CI-OTC-Accounts Receivables Supervisor
CI-OTC-Accounts Receivables Clerk

Using a naming convention such as the business process and job name will make it easier to evaluate later. Using a prefix such as "CI-" will make it easier to filter for all test users. Here's a sneak peek at the dashboard where you can easily identify the test users that are not compliant. From this we can tell that anytime we hire an Accounts Payable Supervisor, risk will be introduced as three of the roles currently granted to this test user have conflicts.



Step 2: Identify and Create Roles

There's a good chance the test users identified will correspond to one or more out-of-the-box roles that Oracle delivers. For example, the roles you assign your test users might look something like this:

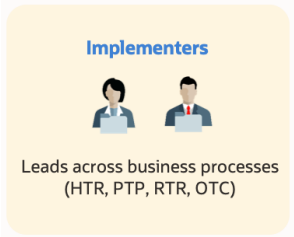
User Name	Assigned Roles
CI-HCM-Human Resource Specialist	• HR Specialist • Employee
CI-PTP-Accounts Payable Supervisor	• Accounts Payable Supervisor • Accounts Payable Manager • Employee
CI-PTP-Accounts Payable Clerk	• Accounts Payable Specialist • Corporate Card Administrator • Employee
CI-PTP-Procurement Agent Buyer	• Supplier Administrator • Procurement Application Administrator • Employee
CI-RTR-General Accountant	• General Accountant • Employee
CI-OTC-Accounts Receivables Supervisor	• Accounts Receivable • General Accounting Manager • Employee
CI-OTC-Accounts Receivables Clerk	• Accounts Receivable Manager • Accounts Receivable Specialist • Employee

There's also a good chance you'll find some SoD conflicts with these delivered job roles. Use the information in the dashboard to optimize these roles, which may entail creating custom roles. The next steps will take you through how that process might look.

Deploy and Run Advanced Access Controls

Overview & Participants

The compliance/internal audit team works with business process owners to identify the initial risks to address and deploy the corresponding access controls.



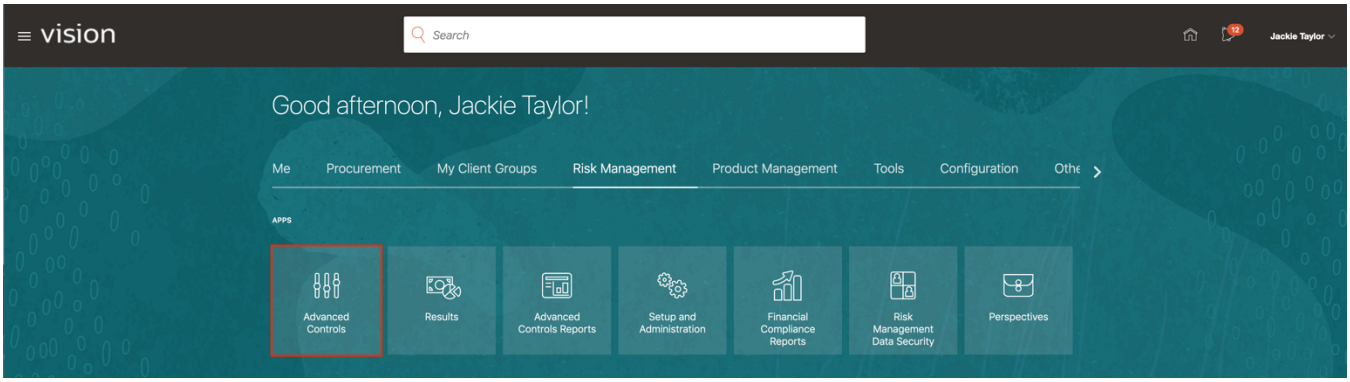
The ERP implementation consultants work with the risk & compliance team to identify appropriate user access and remediation tasks related to user conflicts found.

Step 1: Identify Risks

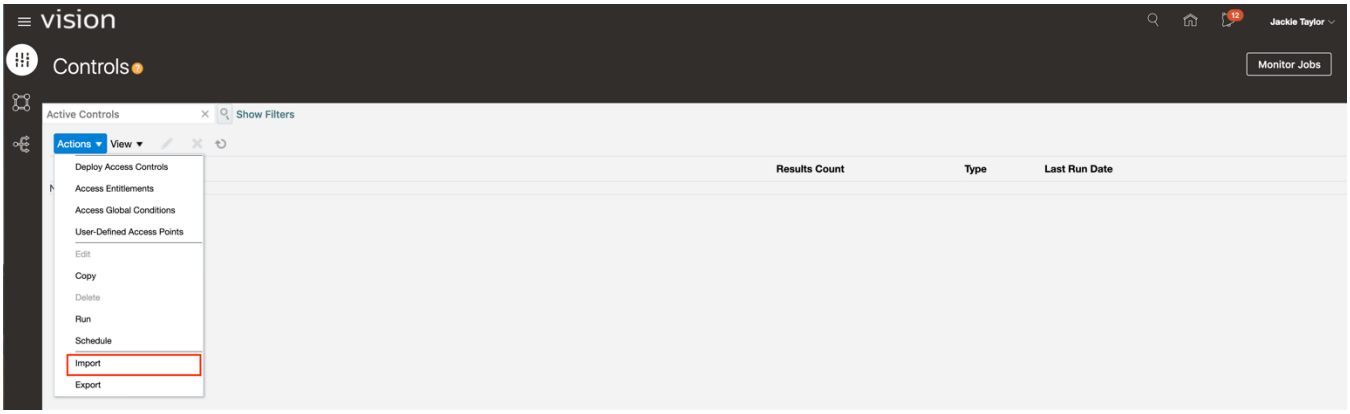
Start with your existing risks based on your interactions with auditors, and map them to our pre-built controls; or deploy the starter pack we provide, which is a subset of our pre-built control library. We've selected controls that are popular because they address risks of cash leaks and financial misstatements.

Step 2: Import Controls

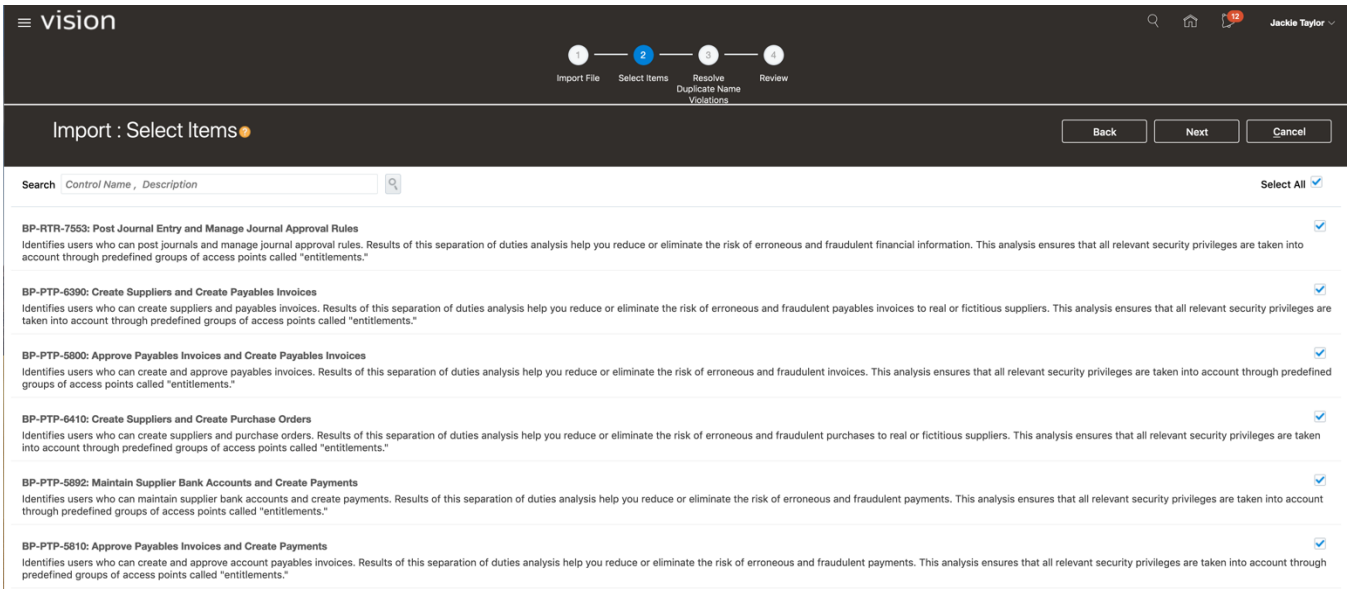
Navigate to Risk Management and click Advanced Controls:



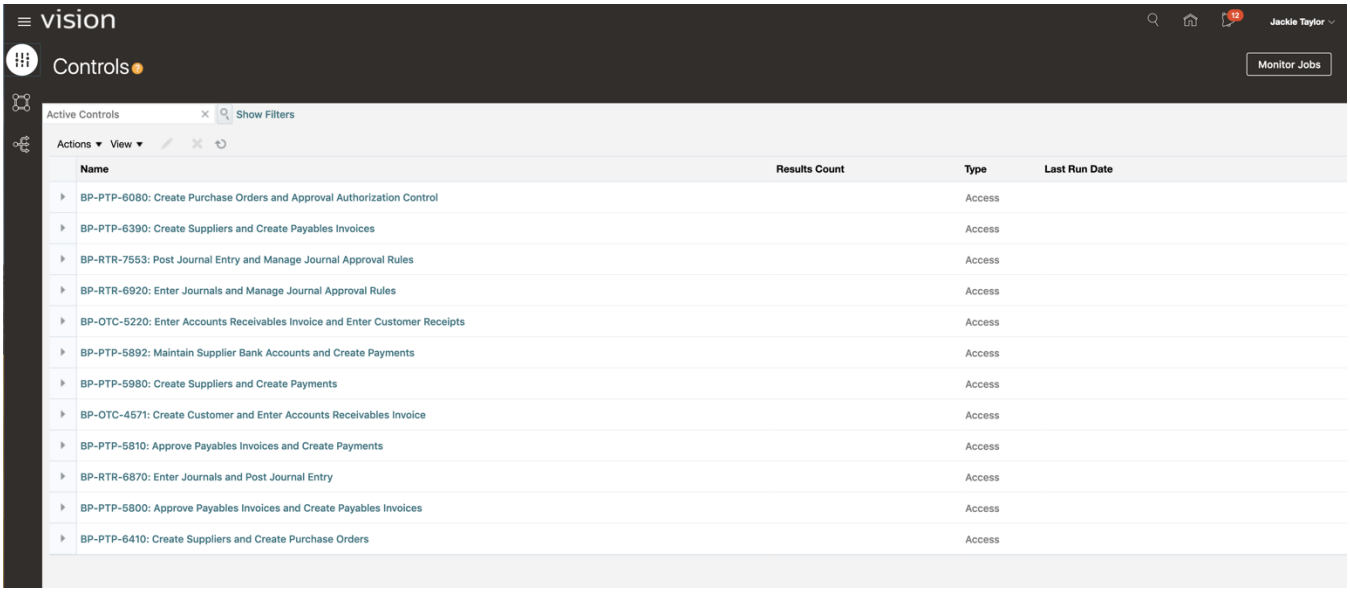
Select Actions > Import and select the 'Top 12 Advanced Access ERP Controls.xml' file: https://cloudcustomerconnect.oracle.com/posts/1aaf01117a



Select Next to move to the Select Items stop. Review the controls and their descriptions. Select the controls that relate to the risks you've identified:



Click Next a couple times to get to the Review stop. Then click Submit. You can monitor jobs to see when the control import job completes, or periodically click the refresh icon on the controls page.

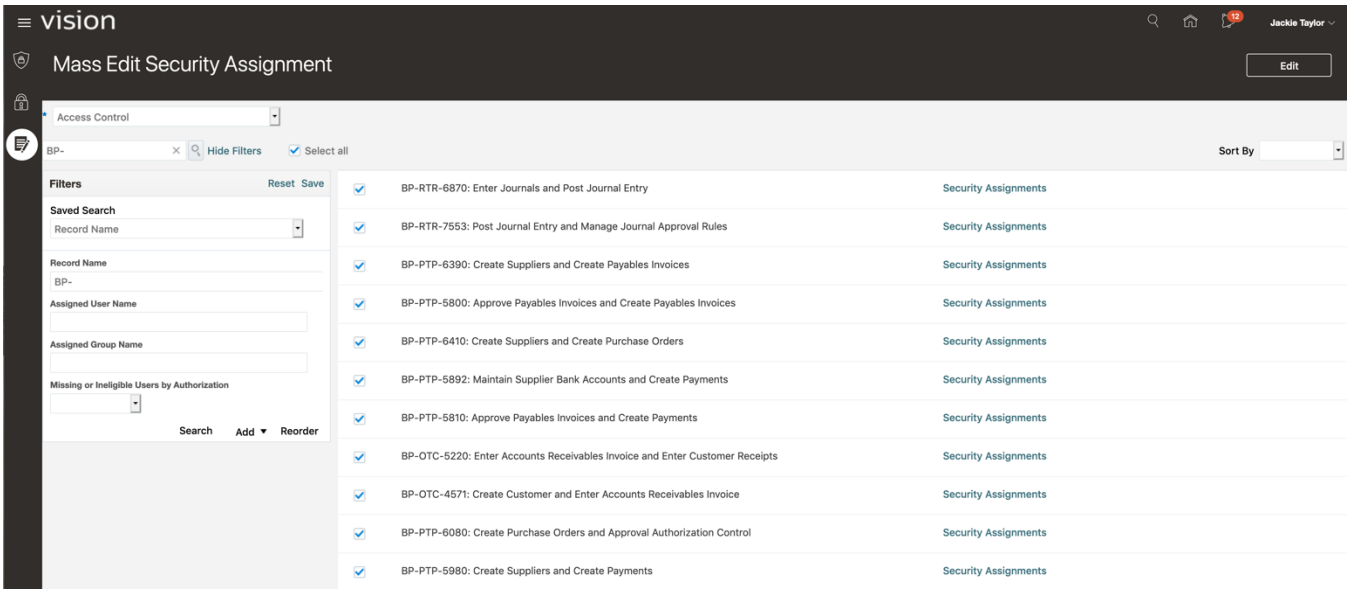


Since you are the one importing the controls, you automatically become their owner. Next you'll add an important user assignment group.

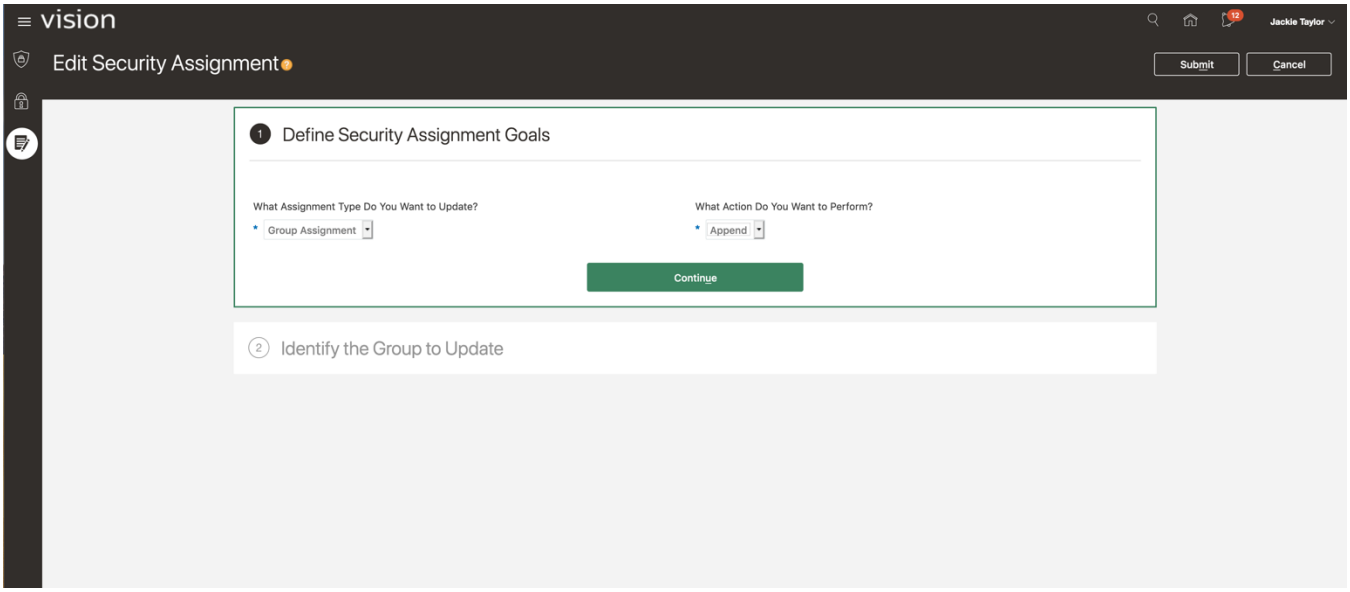
Step 3: Security Assignment – Control

Navigate to Risk Management Data Security > Mass Edit Security Assignment. Select Access Control for the object and search for all controls that begin with “BP-”.

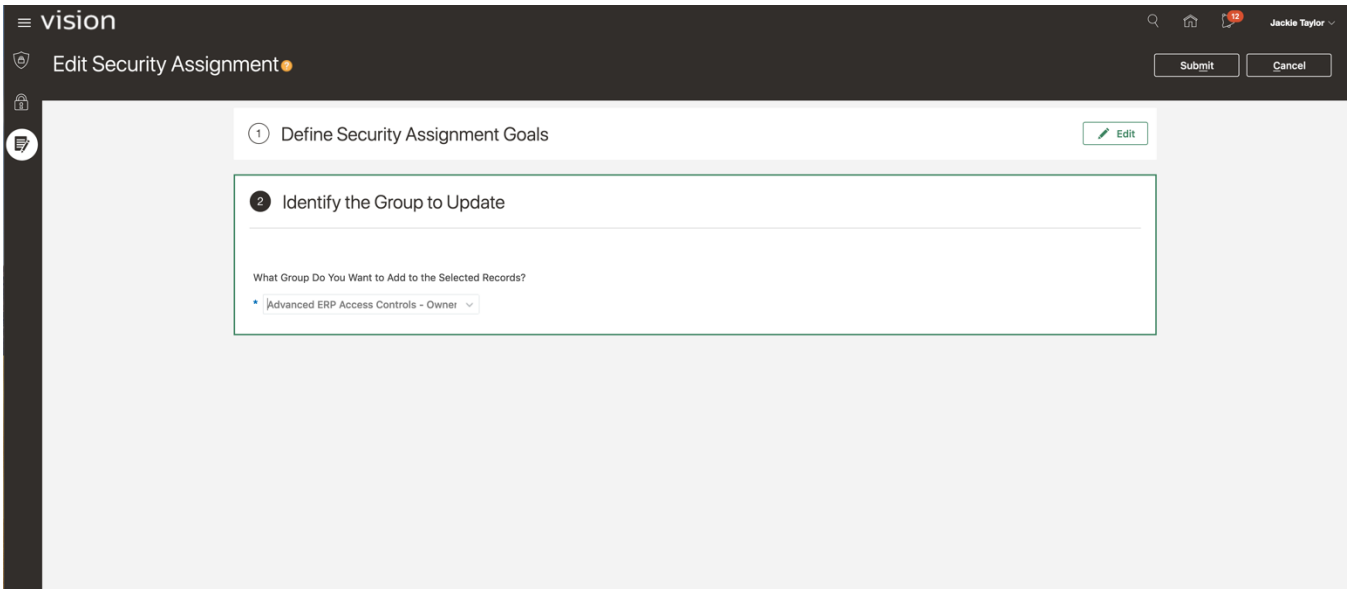
Tick the Select All check box, then click Edit:



Select “Group Assignment” and “Append” from the drop downs, then click Continue:

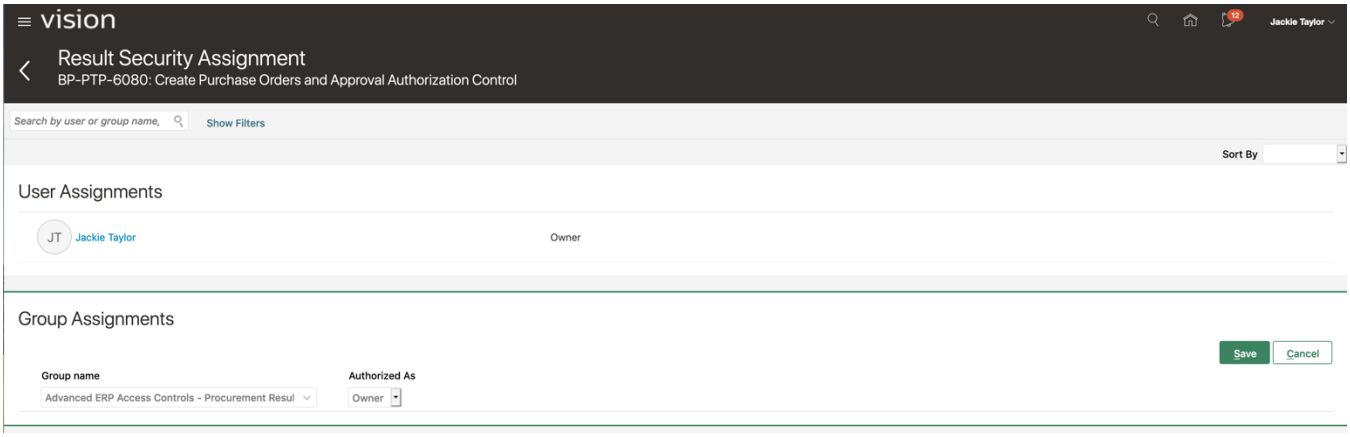


Select the group you created earlier: in this case, ‘Advanced ERP Access Controls – Owner,’ and click Submit:

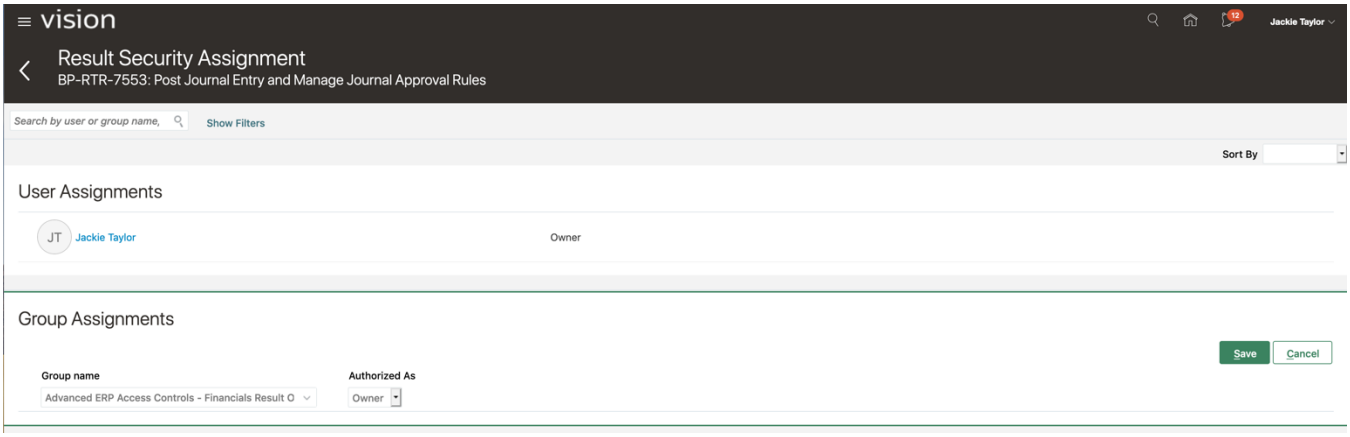


Step 4: Security Assignment – Control Result

Navigate to Risk Management > Advanced Controls. Click on the control name, then select Security Assignment > Result Security Assignment. This is a procurement control, so select the procurement group:



For the financial controls, select the financial group:



Note: We hope to provide the option to mass-assign the same group across a selection of controls in an upcoming release.

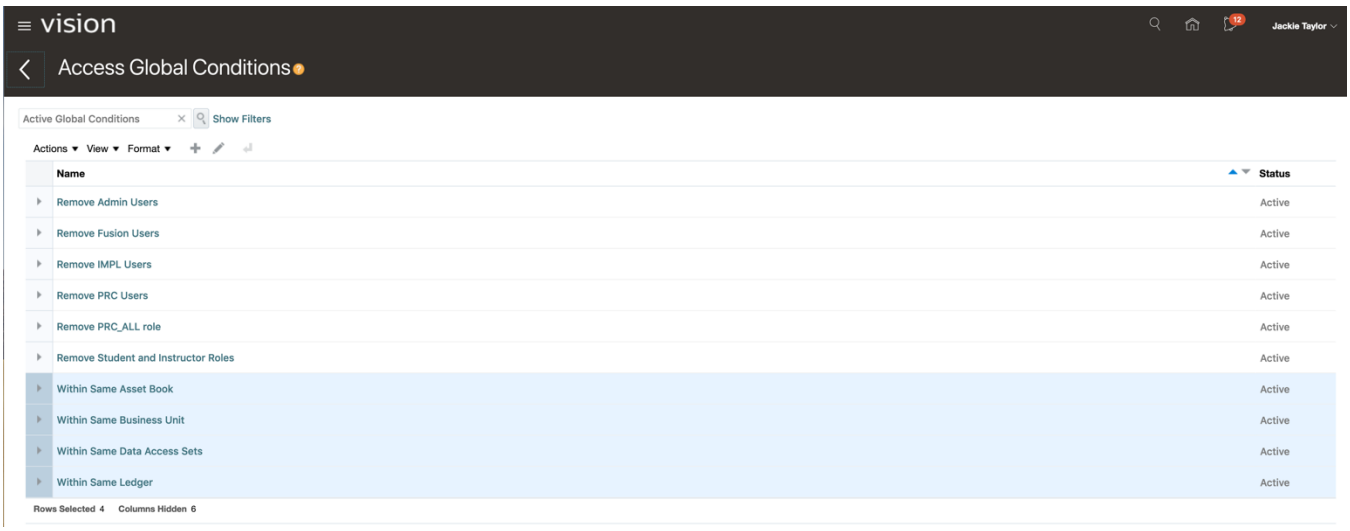
Step 5: Deploy Global Conditions

Navigate to Risk Management > Advanced Controls. Click on Actions > Access Global Conditions. Select Actions > Import and select the "Top 4 Global Conditions.xml" file: https://cloudcustomerconnect.oracle.com/posts/1aaf01117a

These "Within Same" global conditions consider the data security that's set up in the Manage Data Access for Users page. These conditions reduce false positives. For example, if a user has a job role for Accounts Payable Manager that has been assigned data access for business unit BU1, and a job role for Accounts Payable Clerk that has been assigned business unit BU2, then these roles would not be considered in conflict since the business units are not the same. (Only user access where the business units are the same would be considered a conflict.)

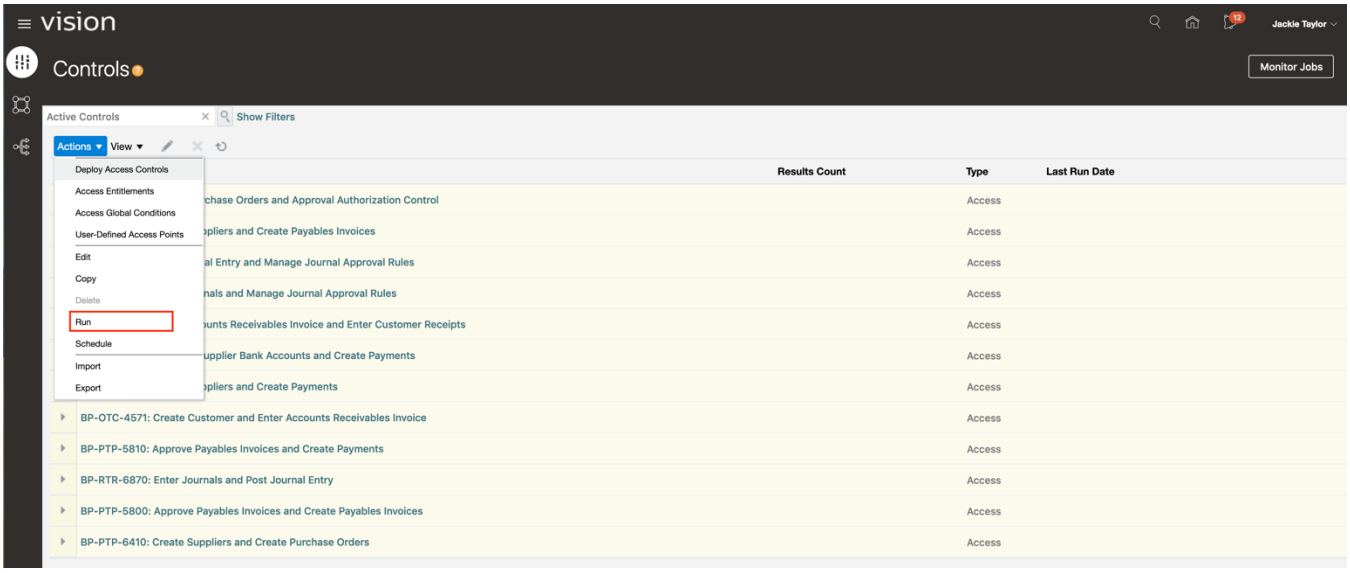
You may also consider adding additional global conditions to exclude known superusers or their roles, especially in a development environment.

Note: Global conditions apply to all controls. If a condition is required for a specific control, import the control as a model and apply the condition there.

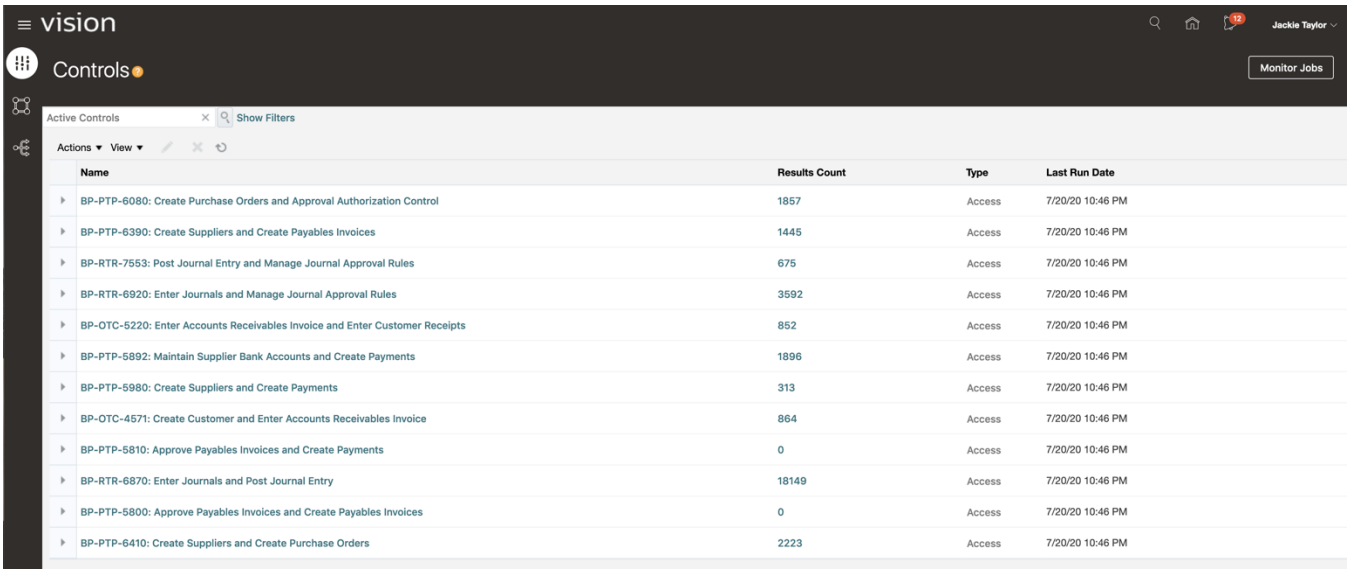


Step 6: Run Controls

Navigate to Risk Management > Advanced Controls. Select the first record and shift+click the last record. Select Actions > Run”

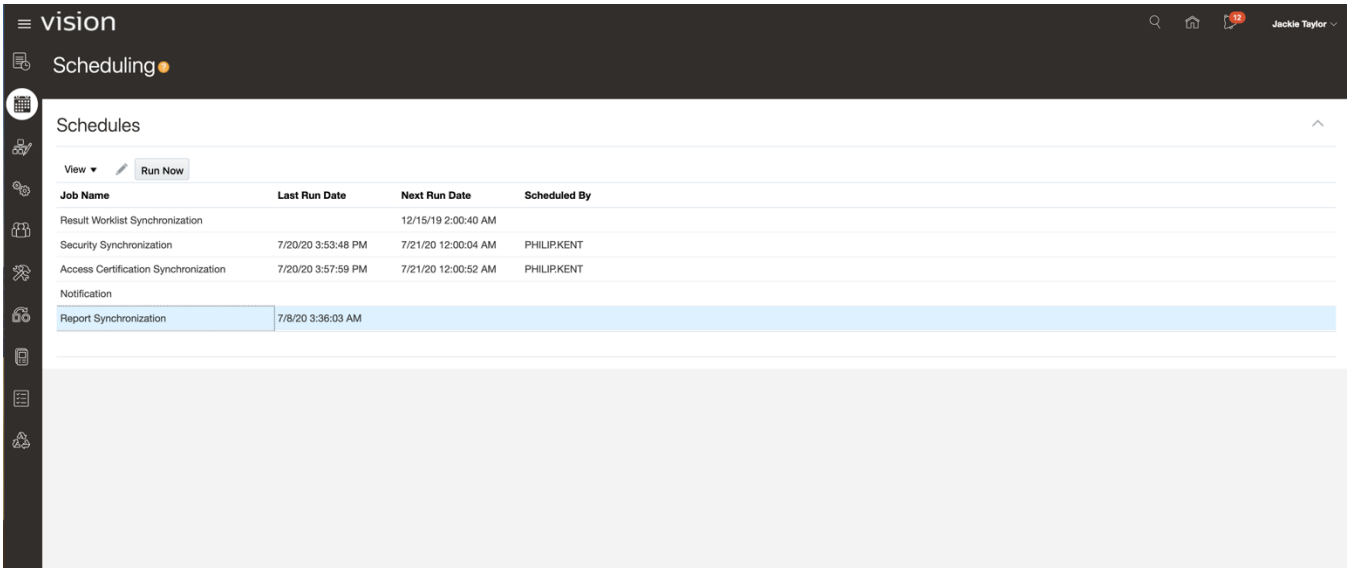


When control analyses have completed, the results counts are populated:



Step 7: Run Report Synchronization

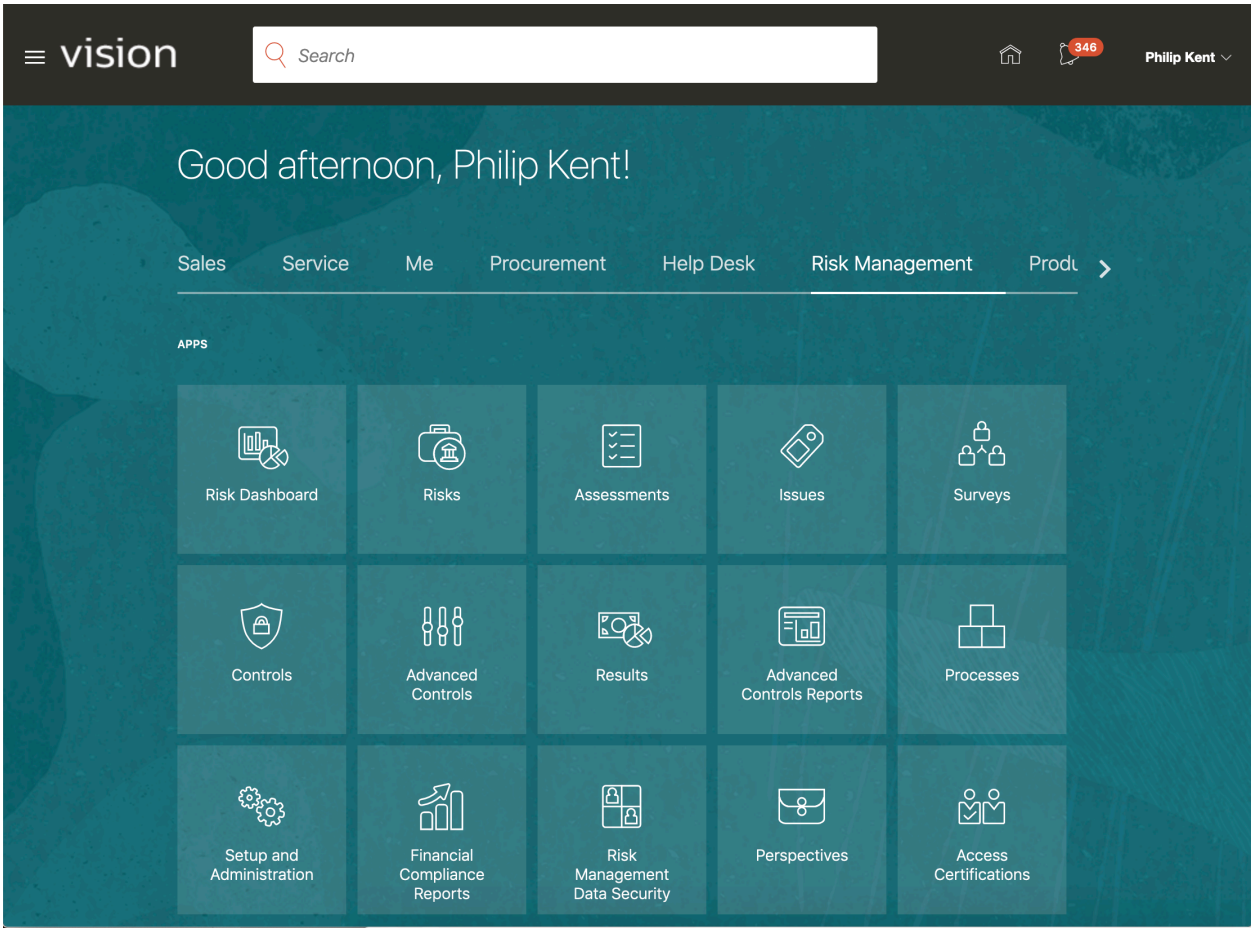
Navigate to Risk Management > Setup and Administration. Select the Scheduling tab, then run Report Synchronization:



View Results and Implement Changes

An ERP implementation timeline can span several months. The workstreams involved for the various business areas will most likely happen at different points in time. In other words, business areas such as Hire to Retire, Procure to Pay, Record to Report and Order to Cash will not all be implemented at the same time, but in phases. At any point in time an ERP implementer involved with security design can leverage the Risk Dashboard for insight into optimizing security design for the business process being implemented.

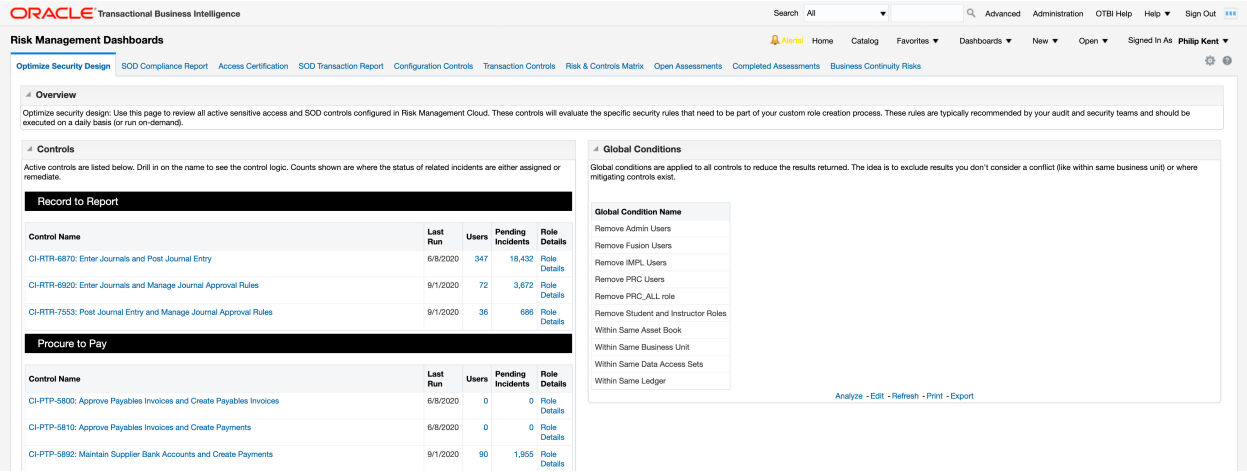
Step 1: Navigate to Risk Dashboard



Step 2: Review Controls & Global Conditions

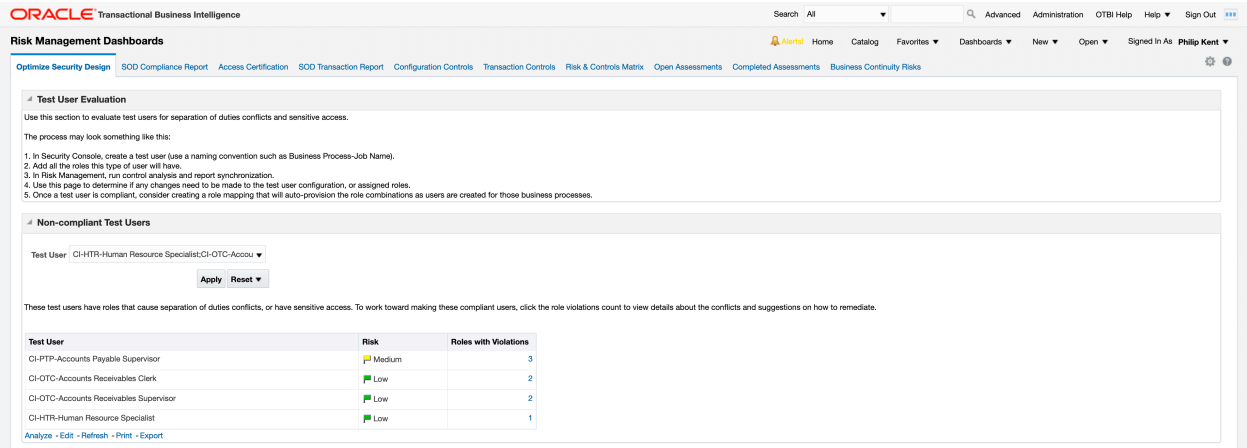
As the overview section in the dashboard describes, use this page to review all active sensitive access and SOD controls configured in Risk Management Cloud. These controls will evaluate the specific security rules that need to be part of your custom role creation process. These rules are typically recommended by your audit and security teams and should be executed on a daily basis (or run on-demand).

Learn more about the control by drilling in on the name. View a distinct list of users or roles with conflicts by clicking on the corresponding count hyperlink. To view and act on the related incidents, drill into the Pending Incidents count.



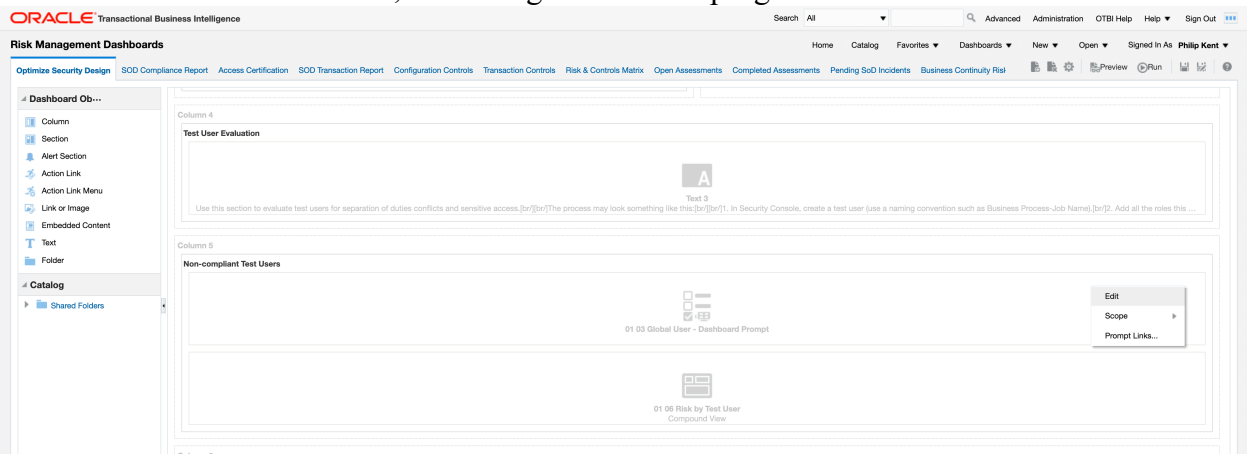
Step 3: Evaluate Test Users

Further down the page you'll see an Evaluate Test User section. As it states, use this page to evaluate test users for separation of duties conflicts and sensitive access. In previous steps, you already created test users and assigned roles to them. You also already ran access controls and report synchronization.

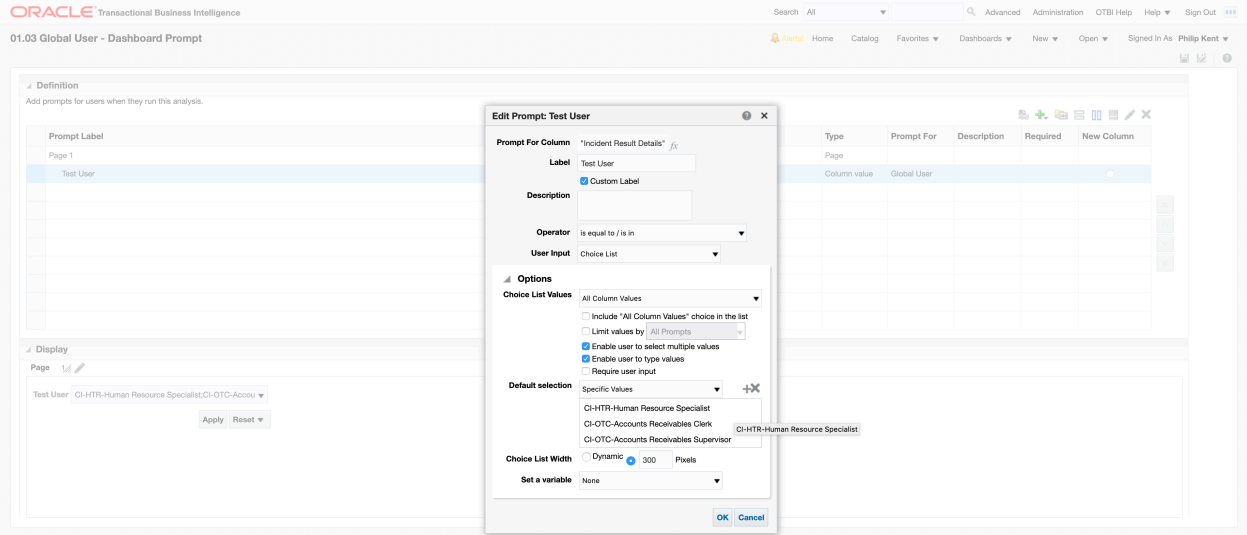


The dashboard by default is only showing users that begin with "CI-". If you used a different naming convention, follow these steps:

1. While in the dashboard, click the gear icon in top right and Edit Dashboard



2. Select the xyz icon in the 01.03 Global User – Dashboard Prompt section and Edit.
3. Select the Test User Prompt Label then select pencil icon in top left.
4. Expand Options section and in Default selection click the plus icon to modify the default values selected.
5. Save your changes and run the dashboard.

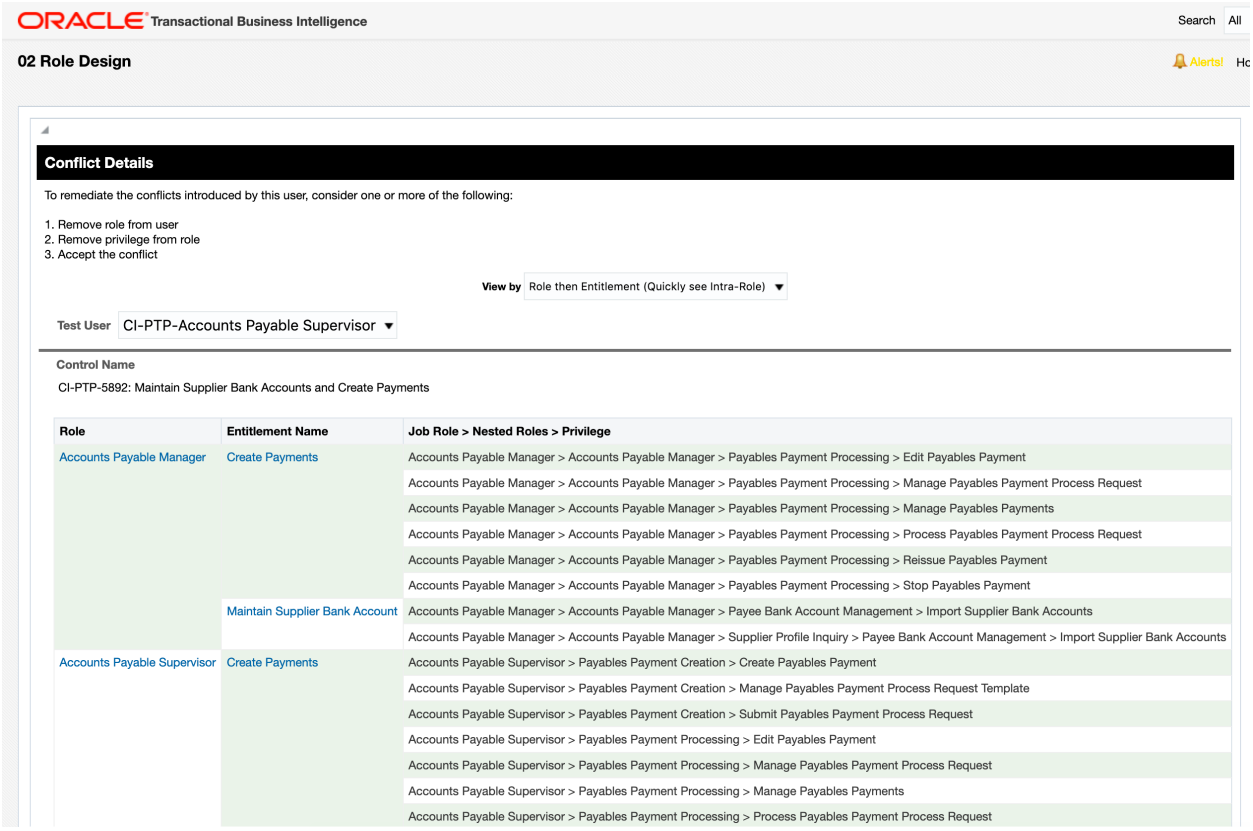


Now you should have data for the test users you created.

Step 4: Evaluate Non-Compliant Test Users

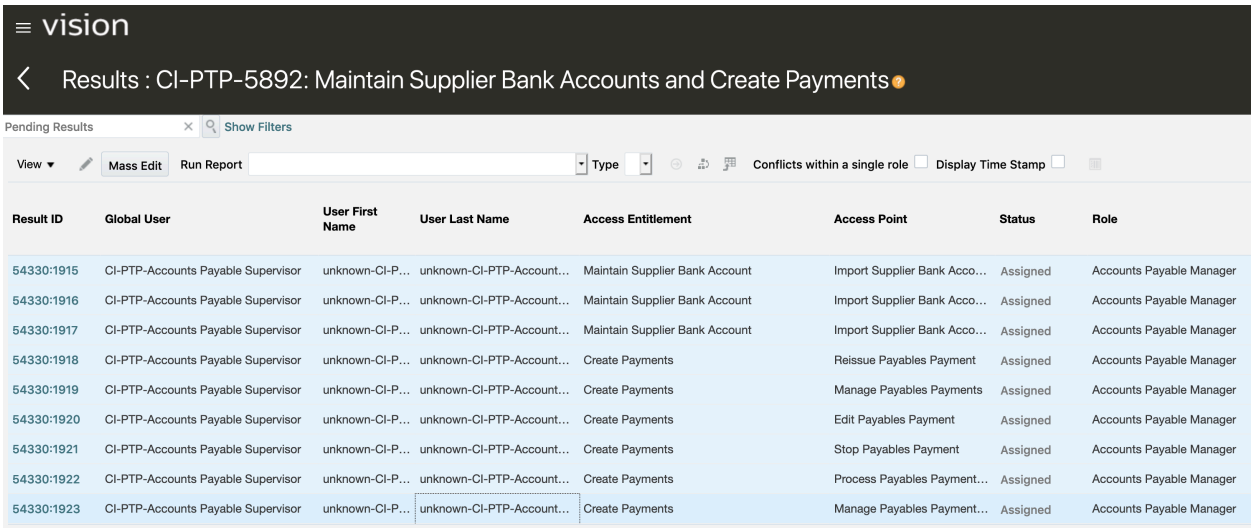
For each non-compliant, drill into the roles with violations. To remediate the conflicts introduced by this user, consider one or more of the following:

1. Remove role from user
2. Remove privilege from role
3. Accept the conflict

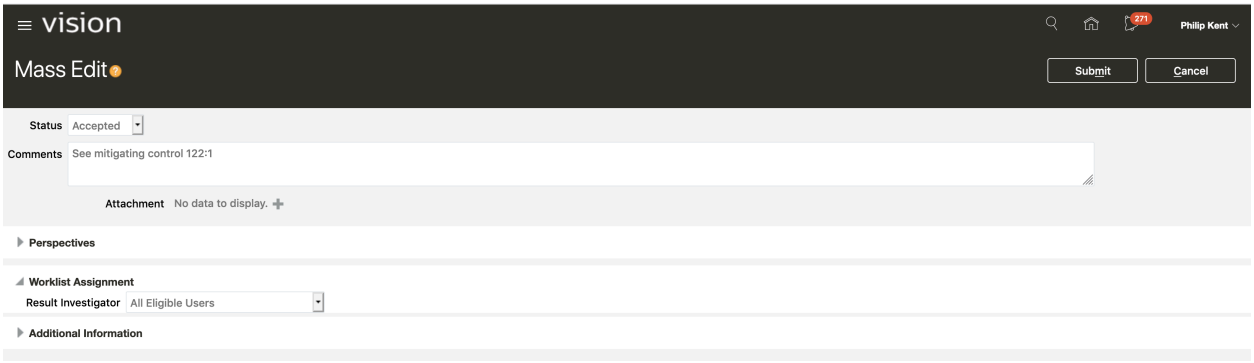


Step 5: Track Remediation Action

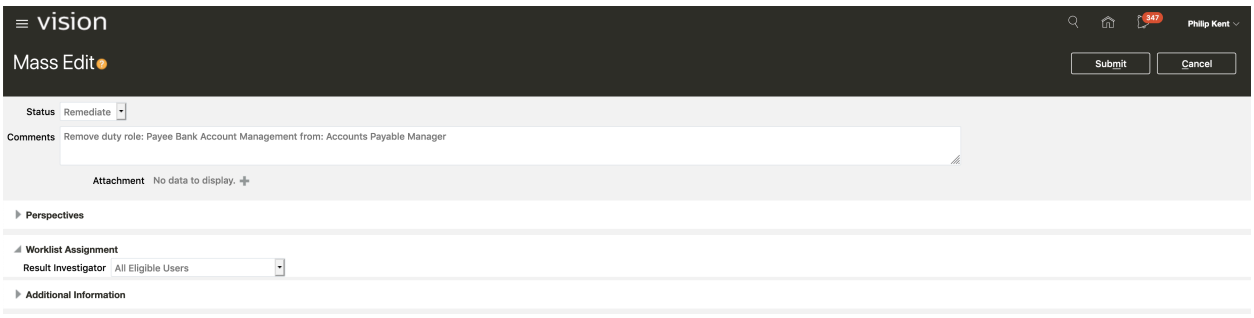
You may find it helpful to track your remediation action on the incidents. For example, click on the role name to drill into the results page for that control, user and role and accept the risk and add a mitigating control.



Note: Use the pencil icon to mass edit selected rows. Use the Mass Edit button to update all records for that control.

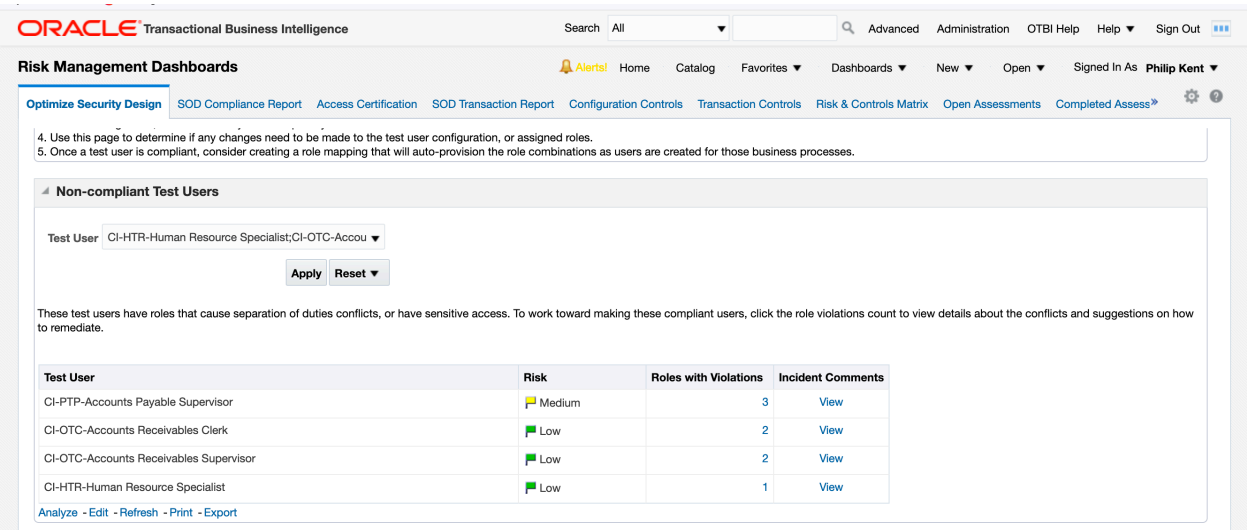


Or, set the status to Remediate and add comments recommending what remediation action to take.

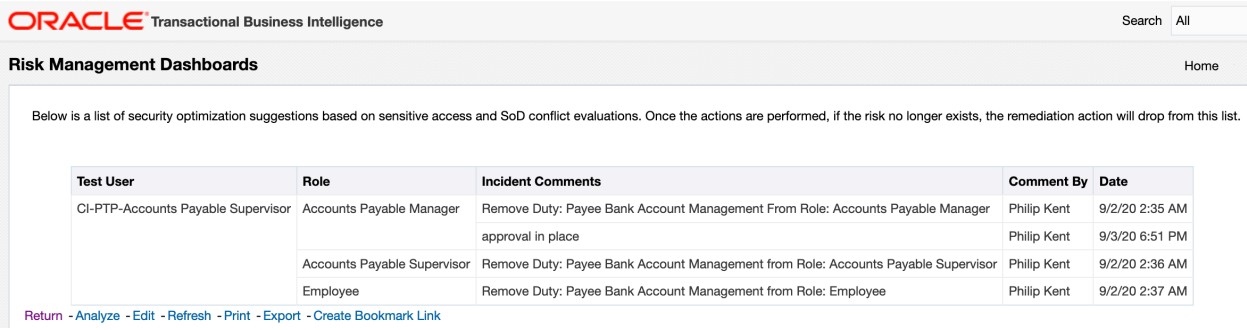


Step 6: Implement Security Optimizations

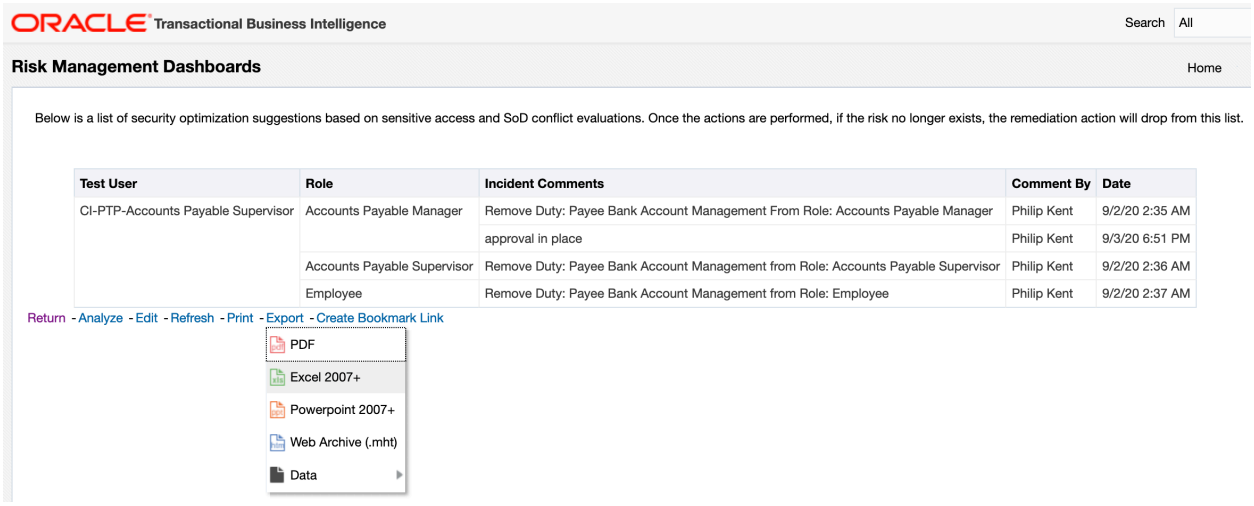
A security administrator can use this same dashboard to methodically work through remediation actions recommended by the business. For each test user, select the view link in the Incident Comments column.



As the security administrator implements these suggestions noted in the incident comments column, and the requisite jobs are run (which should be scheduled to run on a daily basis, or can be run on demand), if the risk no longer exists, the comment will drop from the list.

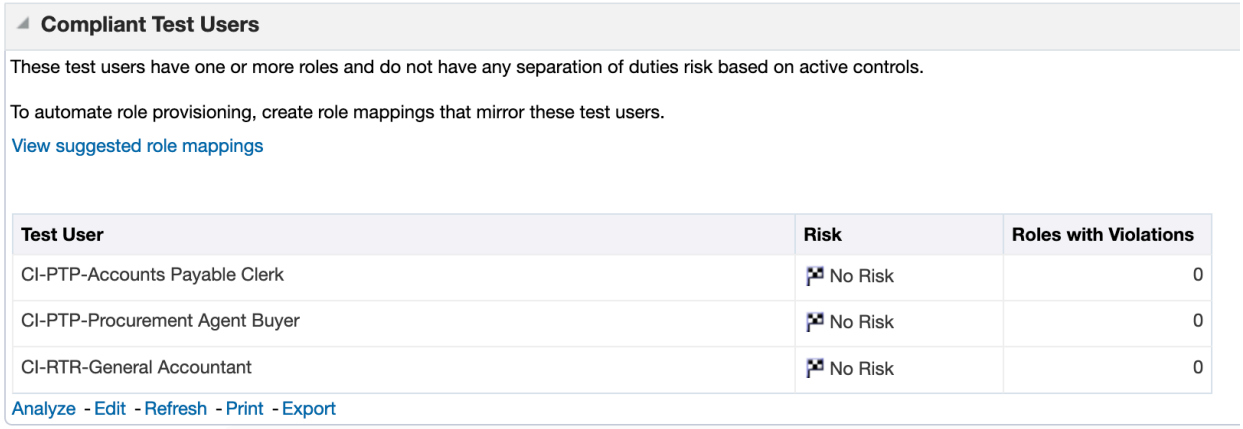


If your company process for requesting changes to security involves a ticketing system, the recommendations can be exported and attached to the ticket you create.



Step 8: Review Compliant Test Users

Once you've gone through this iterative process, the end result is a set of roles that are inherently SoD free, and a set of test users that are compliant (or at least have acceptable, known and mitigated risk).



At this point, you may consider the priority one controls deployed thus far sufficient for optimizing your security design. Consider though, as you deploy additional controls it may come to light that the roles or combination of roles granted to users could be further optimized.

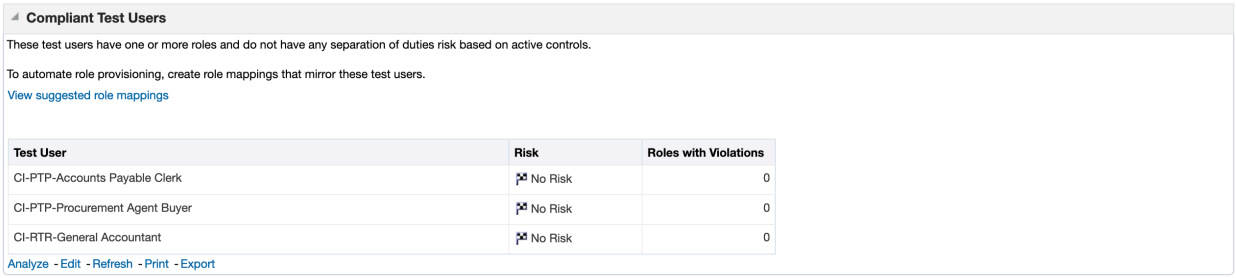
Depending on your timeline and risk appetite, you may consider deploying your priority two controls, and iterating through the process again. You would do this until you have deployed all controls you plan to implement after go-live. This way you will have an opportunity to design the roles and combination of roles granted in such a way that you can feel confident SoD and sensitive access risk is at an acceptable level.

PART 2 – VALIDATE AUTO-PROVISIONING ROLE MAPPINGS

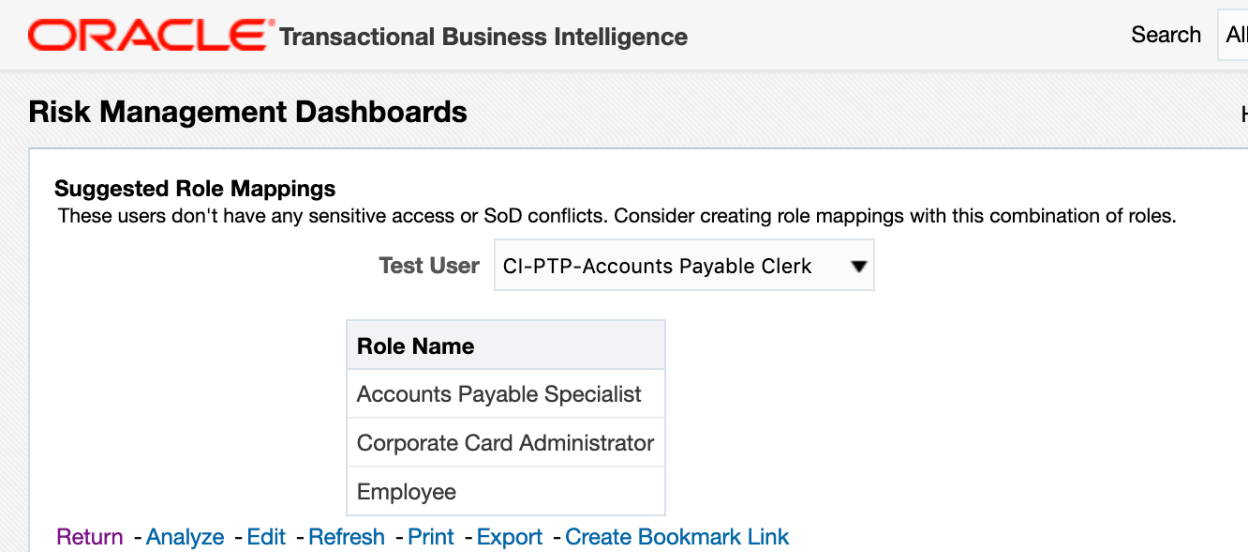
Now that you've cleaned up roles, you're ready to assign those vetted roles and role combinations to real users using auto-provisioning.

Step 1: View Suggested Role Mappings

For example, the test user PTP-Accounts Payable Clerk has no risk, so you can confidently create a role mapping with a combination of roles that matches that test user and know that those roles together do not cause SoD conflicts.



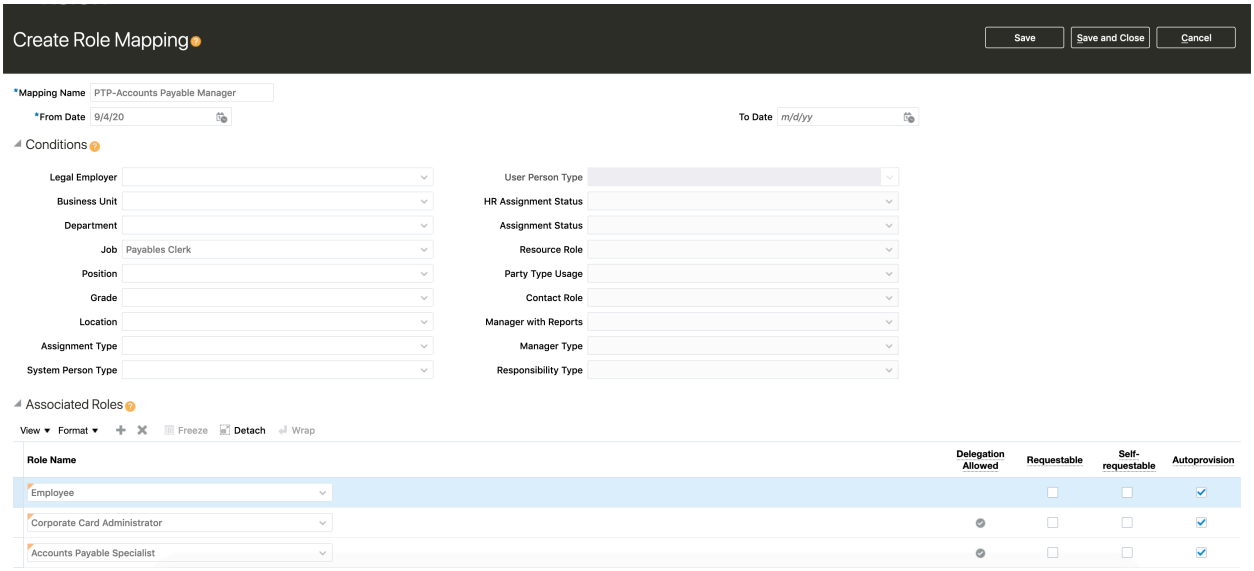
Drill on the View suggested role mapping and select the PTP-Accounts Payable Clerk



Step 2: Set Up Role Mapping

Role provisioning rules, also known as role mappings, determine which data and abstract roles users can have and how they acquire them. During implementation, you create role mappings to provision standard roles, such as Employee and Line Manager, automatically to application users. In addition, you would create the role mappings to include the secure roles you designed in part one of this document.

Navigate to Setup and Maintenance and search for the task Manage Role Provisioning Rules, click the plus icon to create a role mapping. Enter one or more conditions, and the roles to auto-provision when the conditions are met.



See the Application Users section in the Getting Started with Your HR Implementation guide for more information.

Step 3: Create Real Application Users & Auto-provision Roles

Since the assumption is that you are in the midst of an ERP implementation, you will most probably be loading users in bulk. You probably already have employees in another business system that you want to load into Oracle Cloud. If this is the case you can use HCM Data Loader.

Another option to create a user record is during the New Person task flow, such as Hire an Employee or Add a Contingent Worker. By default, human resource specialists and line managers can perform the New Person tasks. Whether user accounts are created for new person records is controlled by the User Account Creation enterprise option.

With either option, when user accounts are created, roles are provisioned to them automatically, as specified by current role mappings.

For more information about application users, roles, and role mappings, see the Securing Oracle HCM Cloud guide. For more information about loading person records in bulk using HCM Data Loader, see the Integrating with Oracle HCM Cloud guide.

Step 4: Run Requisite Jobs

The following jobs will need to run before you'll see the real users in the dashboard. These have all been discussed previously in this document.

- Run the Import User and Role Application Security Data Process
- Run the Security Synchronization Job
- Run the Global User Synchronization Job
- Run Controls
- Run Report Synchronization

Step 5: Review Optimize Security Design Dashboard

By this step, your non-production environment has real application user records with roles assigned. Because those roles were assigned by role mappings which were vetted in part one of this document – you should expect minimal security access risk to be introduced for these real users. Validate that is the case by using the optimize security design dashboard, just as you did in part one. Keep in mind, you'll need to edit the prompt used in the dashboard to remove the "CI-" reference since your real users will not be prefixed in such a way.

If any risk was introduced, you have an opportunity to remediate that before go-live.

PART 3 – USE WEB SERVICES FOR ACCESS/SOD ANALYSIS

If you plan to use a non-Fusion tool (like IDM or a custom provisioning app) to assign roles to users then you should leverage Risk Management APIs to minimize SoD risk as part of this provisioning process. The same Advanced Access Controls configured in part 1 are also available to identify any potential SoD issues. This information can then be used to make an informed, risk-aware decision prior to assigning Fusion roles to a user.

These asynchronous APIs are executed in the following order:

Perform Analysis

- Use this action to initiate a simulation of all active Access Controls configured in Risk Management Cloud.
- The analysis simulates the assignment of Fusion roles and data security context values to a single user.
- No Incidents are created. The results produced by this resource are only a simulation.

Get a Status

- Returns the status of the *Perform Analysis* request above.
- When the status is Completed, call the *Get all results* action below.

Get All Results

- This returns conflicts a user will have if the requested roles and data security context values are assigned to that user.
- Results include the control ID and control name, the requested role and its incident path, as well as the roles with which it conflicts. This is designed to be as complete and semantically equivalent as UI requested analysis (if the role assignments were completed)
- Only potential conflicts resulting directly from the *Perform Analysis* are returned. Existing conflicts for that user are not returned.

Documentation link: https://docs.oracle.com/en/cloud/saas/risk-management/20d/farkm/api-asynchronous-separation-duties-simulations.html

PART 4 – CERTIFY ACCESS

This is a great opportunity to have managers review the roles granted to their staff in a non-production environment. Once certified, you can be that much more confident that users and their security access in the production environment will meet business expectations and SoD risk compliance.

For more information on Access Certification:

- See the user guide: https://docs.oracle.com/en/cloud/saas/risk-management/20c/fauac/index.html
- Consider this Access Certification blueprint: https://cloudcustomerconnect.oracle.com/posts/72c18f17a2

At this point, you may be ready to start migrating your work to production. This decision will likely depend on your company goals and the ERP implementation plan and timeline.

AFTER GO-LIVE

Follow your existing processes related to moving tested configurations, security and data to production. At a high-level, related to the work you've done to optimize security design you'll want to consider:

1. Exporting and importing of security setup data (including custom roles, and role mappings). See Securing HCM documentation: https://docs.oracle.com/en/cloud/saas/human-resources/20c/ochus/export-and-import-of-security-setup-data.html#OCHUS3428915
2. Loading person records, including user records and their associated roles. See the Integrating with Oracle HCM Cloud guide: https://docs.oracle.com/en/cloud/saas/human-resources/20c/faihm/index.html
3. Following the same configuration steps outlined in the getting started portion of this document. If you made any changes to global conditions or controls you will need to create a new export file that can be imported.
4. Running requisite jobs as outlined in this document.
5. Checking the optimize security dashboard.
6. Performing another access certification.

As security artifacts change or new offerings are enabled, be sure to check the optimize security design dashboard before migrating those changes to production to ensure risk is not introduced by role structure or role assignment changes.

RESOURCES: PAPERS, FORUMS AND PRODUCT INFORMATION

Customer Connect Forum:
https://cloudcustomerconnect.oracle.com/resources/081926cc0a/summary

OTBI Dashboards Archive
https://cloudcustomerconnect.oracle.com/posts/26e241d71a

Risk Management Documentation
https://docs.oracle.com/en/cloud/saas/risk-management/20b/fafrc/risks.html#FAFRC1528809

CRITICAL SOD CONTROLS

There are over 130 ERP SoD and sensitive access controls to choose from. This step by step document considers 12 critical controls that address high-risk activities in Payables, Purchasing, General Ledger and Receivables. The control and their corresponding risk statements follow.

Payables

5800: Approve Payables Invoices and Create Payables Invoices

- **Risks to be addressed:** When a user creates an AP invoice record, then approves it, the user's intent could be to allow purchases outside policy.
- **How Advanced Controls addresses risks:** Identifies users who can create and approve payables invoices. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent invoices. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

5810: Approve Payables Invoices and Create Payments

- **Risks to be addressed:** When a user creates an AP invoice record, then creates a supplier payment record, the user's intent could be to create payments for corporate purchases that were not ordered or received.
- **How Advanced Controls addresses risks:** Identifies users who can approve accounts payables invoices and create payments. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent payments. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

5892: Maintain Supplier Bank Accounts and Create Payments

- **Risks to be addressed:** When a user changes a supplier's bank account information, then creates a supplier payment record, the user's intent could be to direct payment to an unauthorized account.
- **How Advanced Controls addresses risks:** Identifies users who can maintain supplier bank accounts and create payments. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent payments. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

5980: Create Suppliers and Create Payments

- **Risks to be addressed:** When a user creates a supplier record, then creates a payment record for that supplier, the user's intent could be to let the supplier obtain payment without providing goods/services, and/or create the appearance of suppliers and/or corporate purchases that do not exist.

- **How Advanced Controls addresses risks:** Identifies users who can create suppliers and payments. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent payments. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

6390: Create Suppliers and Create Payables Invoices

- **Risks to be addressed:** When a user creates a supplier record, then creates an AP invoice record for that supplier, the user's intent could be to let the supplier obtain payment without providing goods/services, and/or create the appearance of suppliers and/or corporate purchases that do not exist.
- **How Advanced Controls addresses risks:** Identifies users who can create suppliers and payables invoices. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent payables invoices to real or fictitious suppliers. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

Purchasing

6080: Create Purchase Orders and Define Procurement Approval Routing Rules

- **Risks to be addressed:** When a user defines an approval routing rule record for purchase orders, then creates a purchase order record, the user's intent could be to order purchases outside of policy.
- **How Advanced Controls addresses risks:** Identifies users who can create purchase orders and define procurement approval routing rules. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent purchases. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

6410: Create Suppliers and Create Purchase Orders

- **Risks to be addressed:** When a user creates a supplier record, then creates a purchase order record for that supplier, the user's intent could be to let the supplier obtain payment without providing goods/services or by providing unwanted goods/services, and/or create the appearance of suppliers and/or corporate purchases that do not exist.
- **How Advanced Controls addresses risks:** Identifies users who can create suppliers and purchase orders. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent purchases to real or fictitious suppliers. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

General Ledger

6870: Enter Journals and Post Journal Entry

- **Risks to be addressed:** When a user creates a journal entry, then posts that entry, the user's intent could be to create the appearance of a financial transaction or adjustment that does not exist.
- **How Advanced Controls addresses risks:** Identifies users who can create and post journals. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent financial information. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

6920: Enter Journals and Manage Journal Approval Rules

- **Risks to be addressed:** When a user defines an approval rule record for journal entries, then creates an entry, the user's intent could be to create entries outside of policy, and/or to create the appearance of a financial transaction or adjustment that does not exist.
- **How Advanced Controls addresses risks:** Identifies users who can enter journals and manage journal approval rules. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent financial information. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

7553: Post Journal Entry and Manage Journal Approval Rules

- **Risks to be addressed:** When a user defines an approval rule record for a journal entry, then posts the entry, the user's intent could be to allow entries outside of policy, and/or to create the appearance of a financial transaction or adjustment that does not exist.
- **How Advanced Controls addresses risks:** Identifies users who can post journals and manage journal approval rules. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent financial information. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

Receivables

4571: Create Customer and Enter Accounts Receivables Invoice

- **Risks to be addressed:** When a user creates a customer record, then creates an AR invoice record for that customer, the user's intent could be to let the customer obtain goods/services outside policy, or create the appearance of customers and/or sales that do not exist.
- **How Advanced Controls addresses risks:** Identifies users who can manage both customers and accounts receivables invoices. Results of this separation of duties analysis help you reduce or eliminate the risk of incorrect sales credit limits, erroneous and fraudulent sales bookings, invoicing, etc. to real or ghost customers. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

5220: Enter Accounts Receivables Invoice and Enter Customer Receipts

- **Risks to be addressed:** When a user creates an AR invoice record, then creates a customer receipt record, the user's intent could be to create refunds for customer purchases that were not made.
- **How Advanced Controls addresses risks:** Identifies users who can manage both enter accounts receivables invoices and enter customer receipts. Results of this separation of duties analysis help you reduce or eliminate the risk of erroneous and fraudulent invoices that may lead to cash leakage. This analysis ensures that all relevant security privileges are considered through predefined groups of access points called "entitlements."

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com  facebook.com/oracle  twitter.com/oracle