ORACLE

Automate Separation of Duties Compliance Reporting

Step-by-step guide to deploying SoD compliance reporting in days

December 2020 | Version 2.0

SUMMARY

If your company is like most, it already has a process for generating separation of duties (SoD) reports periodically – often quarterly. For many companies the process involves spreadsheets, custom tools and consultants – things that make it time-intensive, inefficient and costly.

This document gives step-by-step instructions for trading up to an automated process that will:

- Generate compliance-driven SoD reports with confidence each quarter
- Reduce audit effort and consulting fees
- Quickly tailor SoD reports and dashboards using embedded tools
- Eliminate the risks of copying and distributing sensitive ERP security data, as required by third-party systems or external consultants
- View SoD results in minutes using a pre-built library of best-practice rules
- Leverage our easy-to-use visual workbench to tailor those rules and create your own

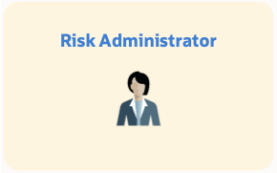
PREPARE IN A NON-PRODUCTION ENVIRONMENT

Start in a non-production environment. Once you're satisfied with the initial set of controls and results, migrate to production.

Prerequisites

Overview & Participants

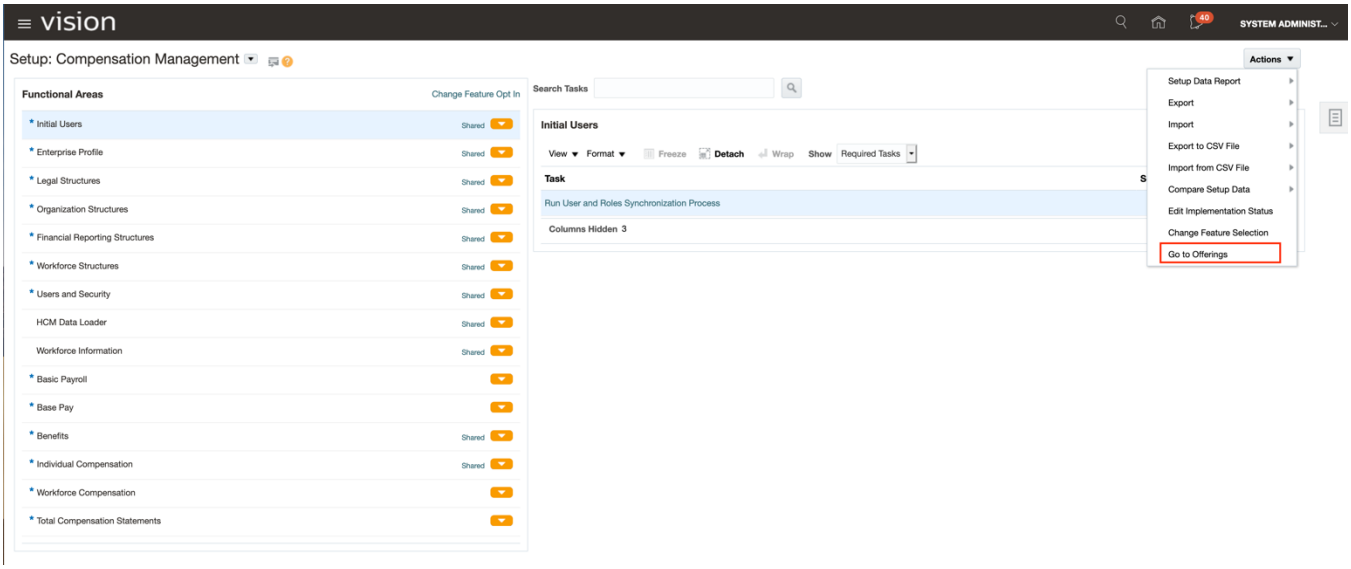
Your security team will enable the Risk Management offering and grant access to the compliance team and business process owners who will set up the automation and review SoD conflicts.



Your risk administrator will run various jobs and deploy your Risk Management dashboard.

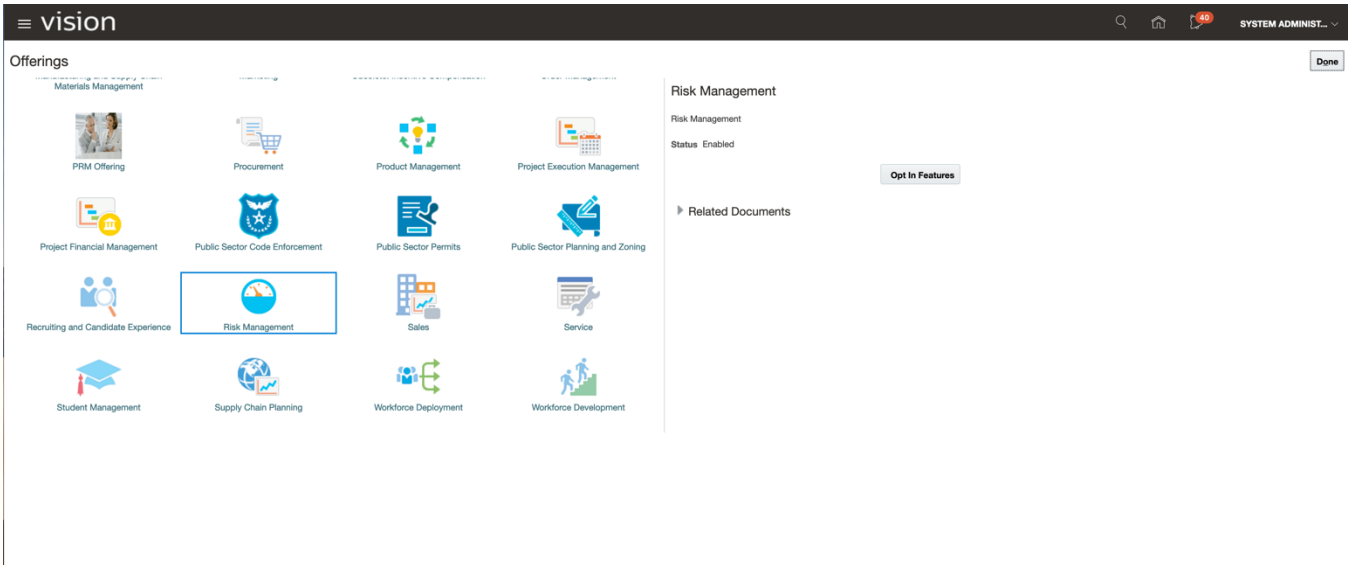
Step 1: Activate Risk Management

Your first step is to make sure Risk Management is activated in your instance. 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’:



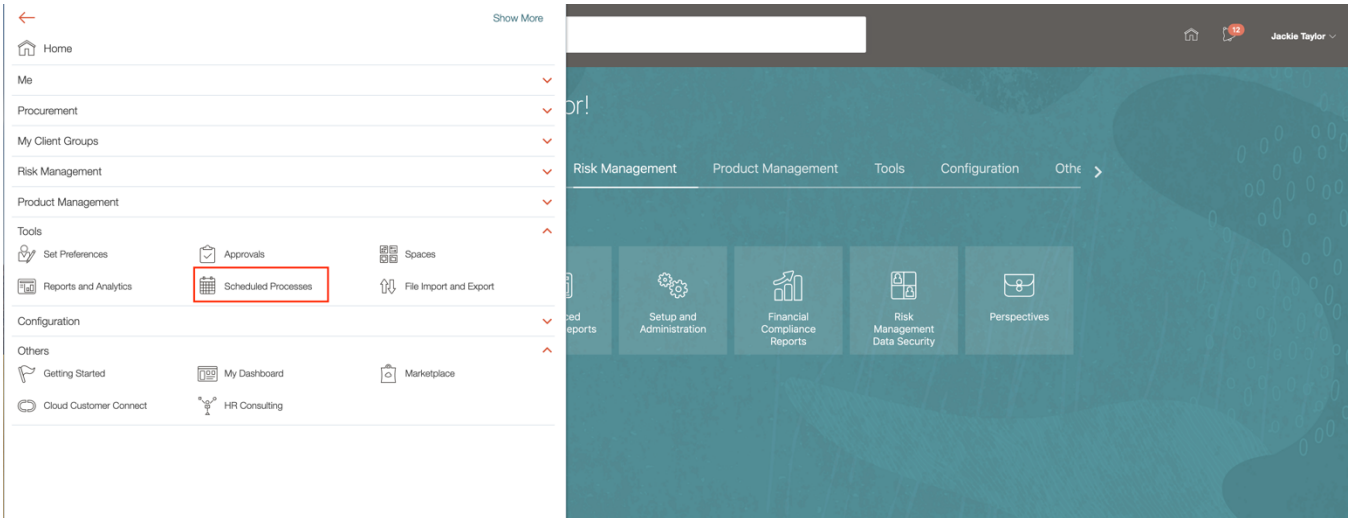
Step 2: Assign Risk Management Job Roles

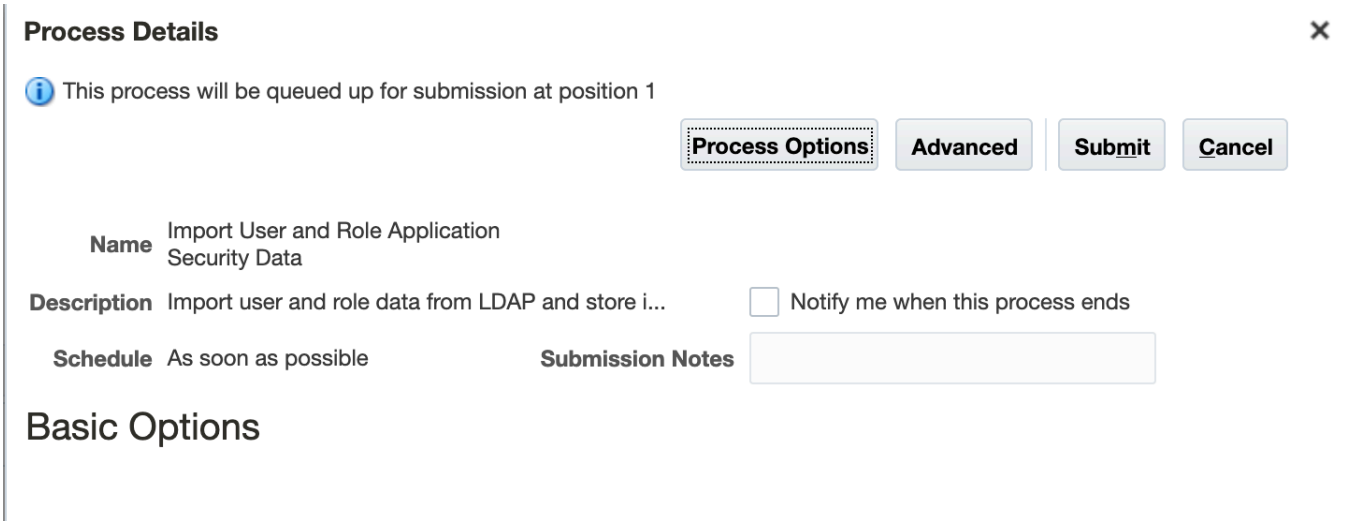
Assign your compliance team members the following job roles:

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.

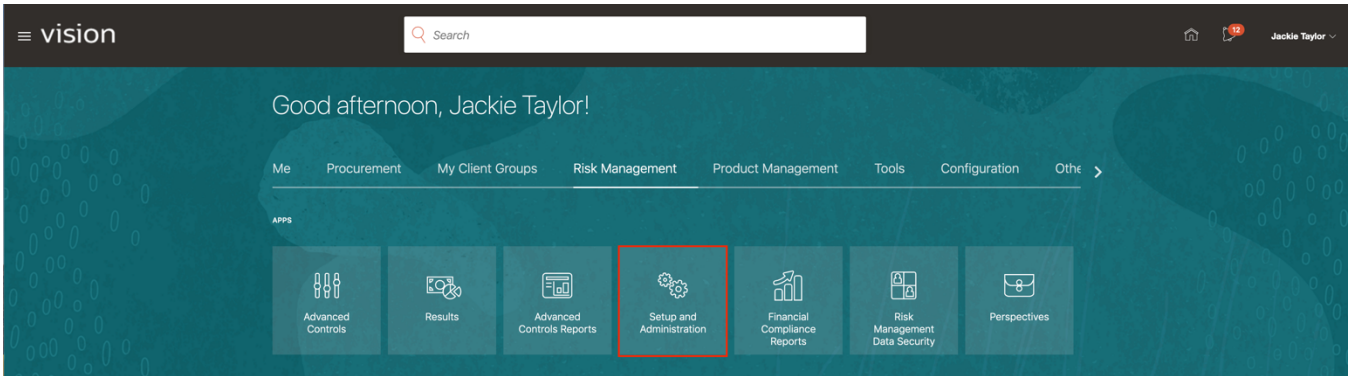


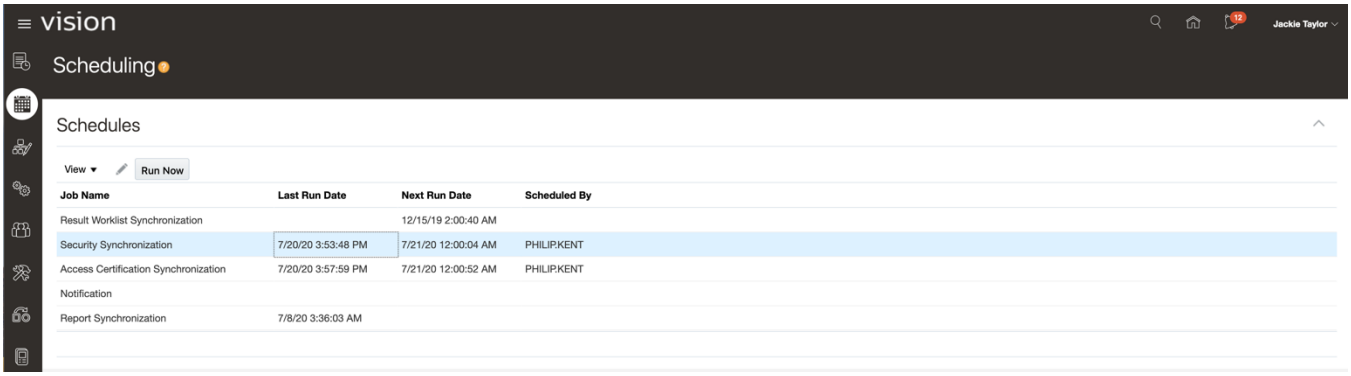


Step 4: Run the Security Synchronization Job

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.

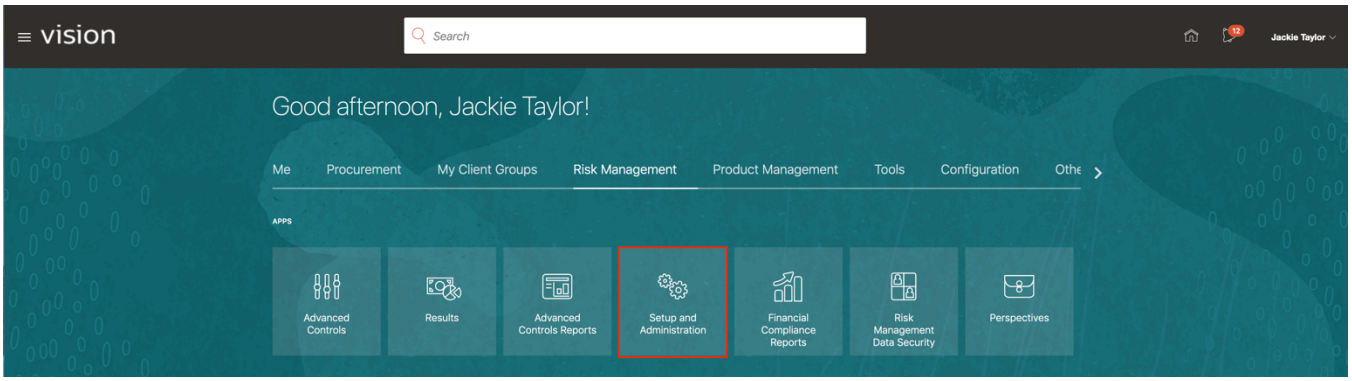
Navigate to Risk Management > Setup and Administration, then click the Scheduling tab:



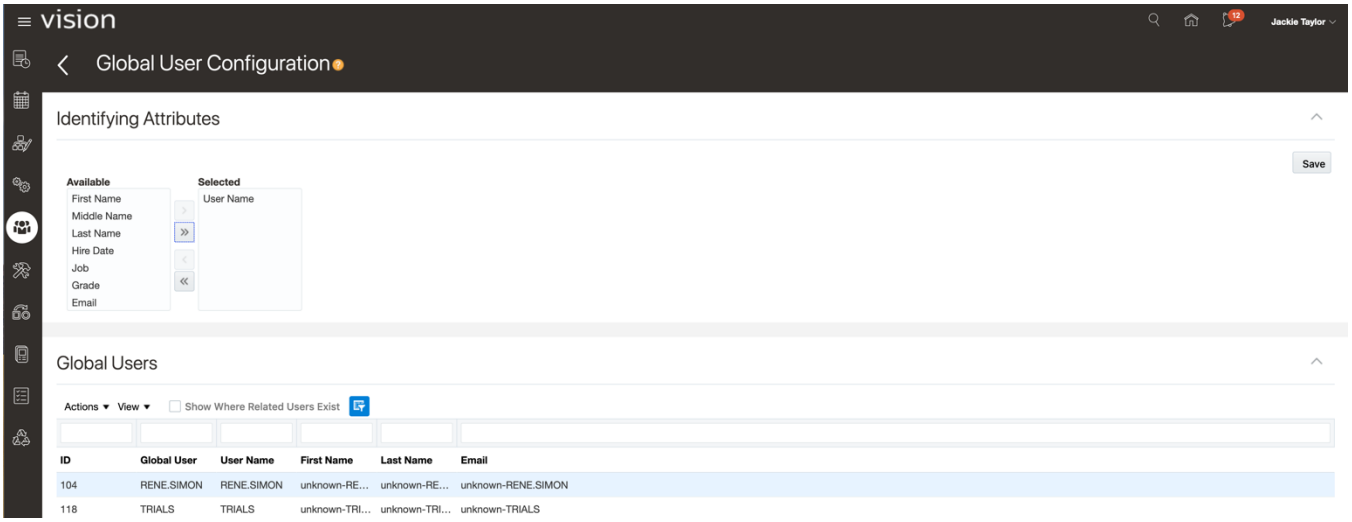


Step 5: Configure Global Users and Run the Global User Synchronization Job

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:

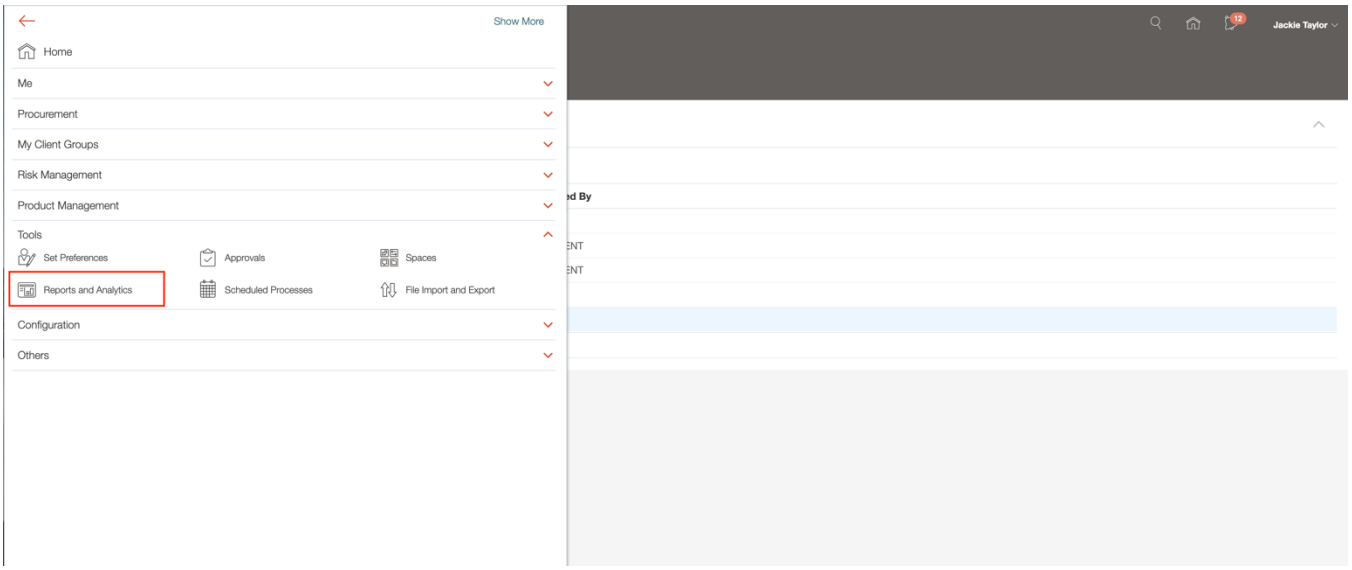


Once that job completes, the Global Users section is populated. These are users synchronized from the Users area in Security Console. The job role assignments for these users will be evaluated during control analysis, and the global user name is the value associated to incidents identified.

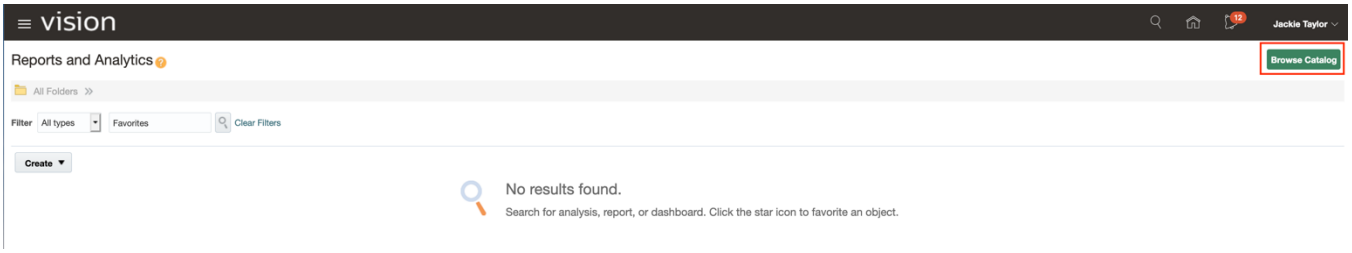
Step 6: Deploy the Risk Management Dashboard

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.

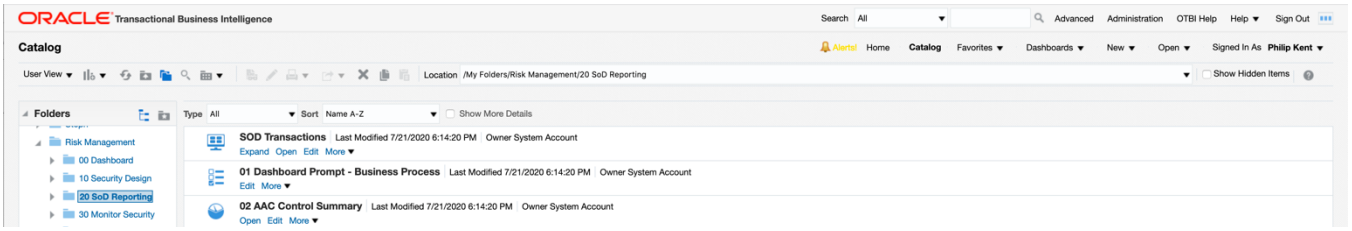
Navigate to Reports and Analytics, then select Browse Catalog:



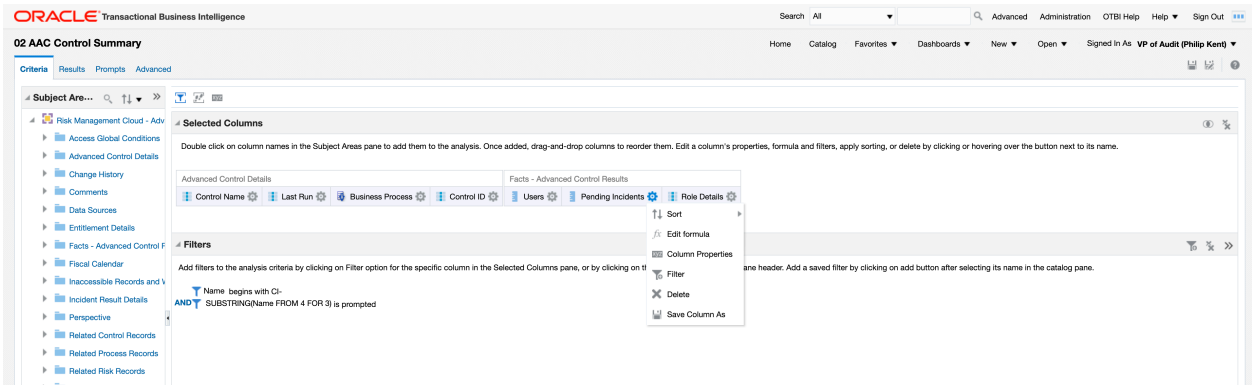
Under Shared Folders, select Custom. Unarchive our Solution Blueprint Risk Management catalog: https://cloudcustomerconnect.oracle.com/posts/6ac0498b5e; that will create a Risk Management folder. Select "00 Dashboard," then click edit on the Risk Management Dashboards:



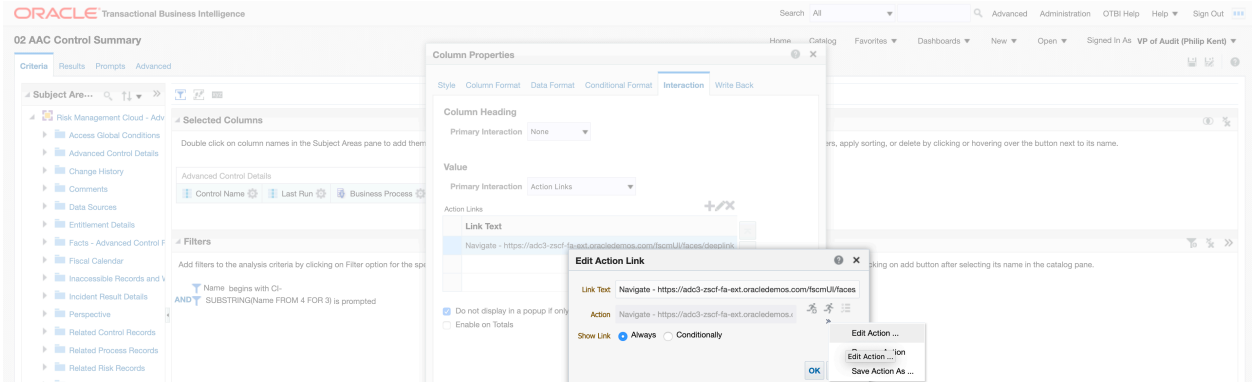
Edit the "02 AAC Control Summary" analysis found in the "Risk Management > 20 SoD Reporting" folder:



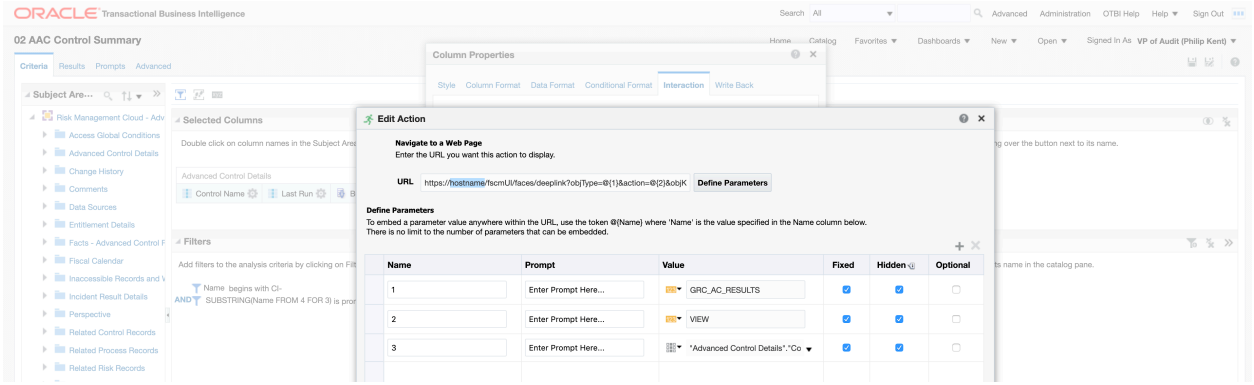
Click the gear box on the Pending Incidents column and select column properties:



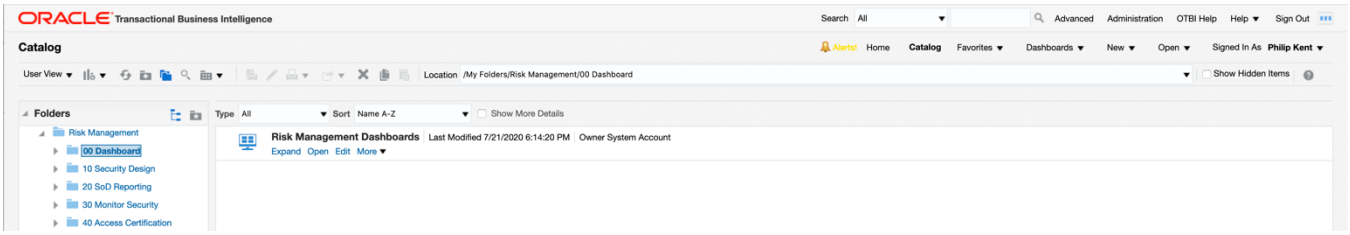
Edit the action link URL:



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

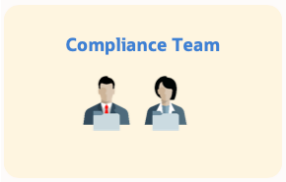


Save the report and run the dashboard by navigating to the “00 Dashboard” and click on Open for the “Risk Management Dashboards”:



Create User Assignment Security Groups

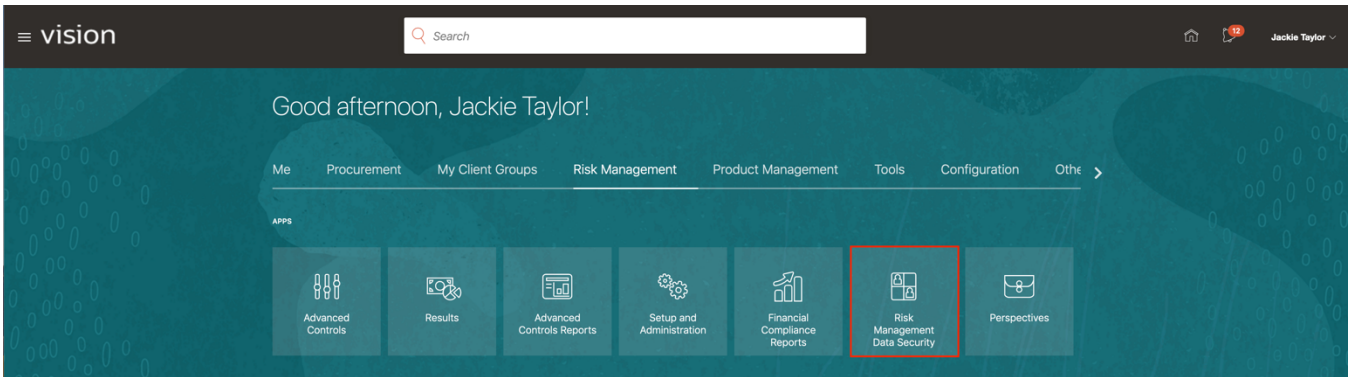
Overview & Participants



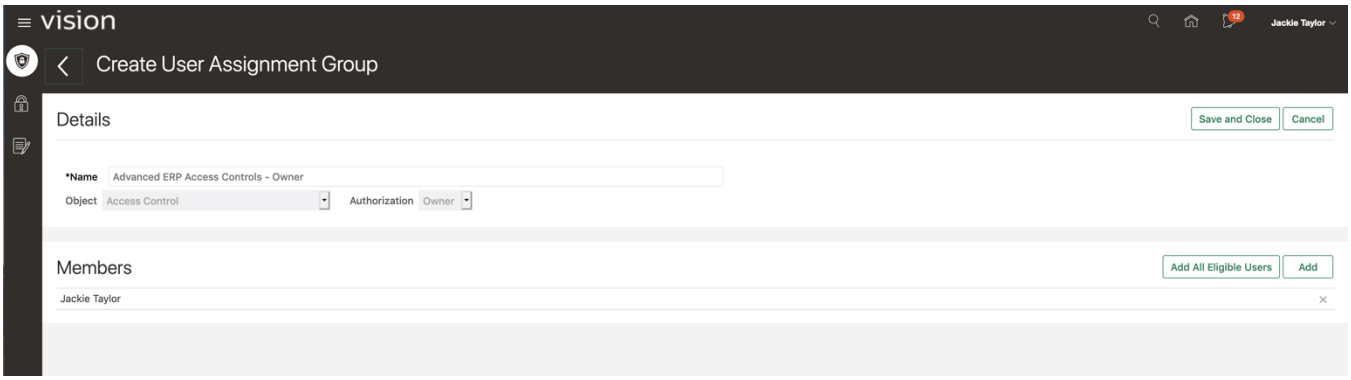
The most scalable approach to setting up security in Risk Management is to create a user assignment group, even if only one person is in that group. Later, if you need to add or change a group's members, it's easy.

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":

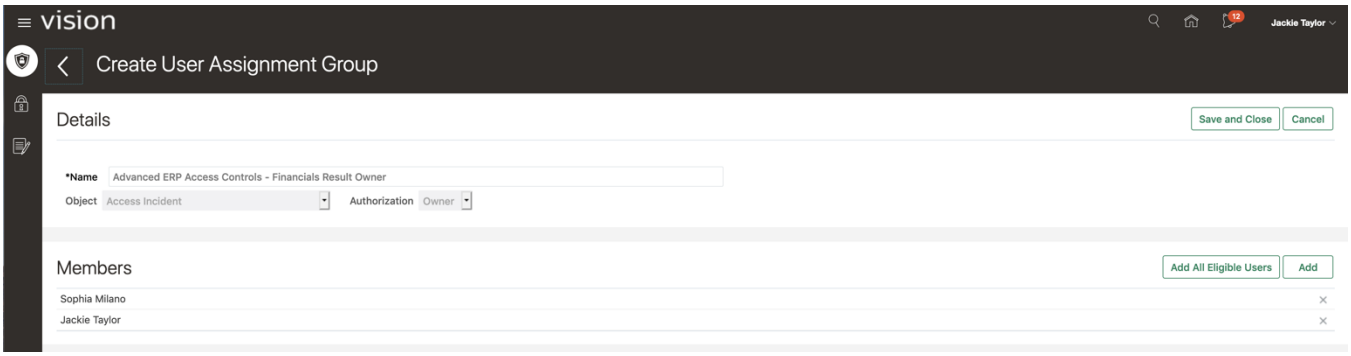


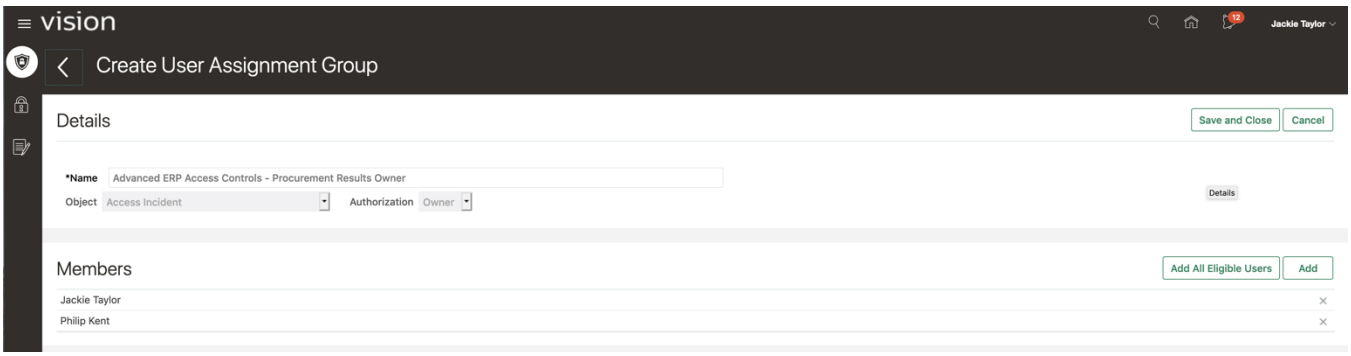
In the Members section, click Add and select one or more members. These are people who will be able to view, edit and assign security to access control records. For now, this is sufficient. As your project evolves, you may decide to add additional user assignment groups where members are only authorized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

Step 2: Create User Assignment Group for Control Results

Navigate to Risk Management > Risk Management Data Security.

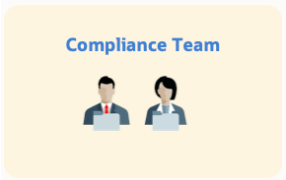
For each control, you can set the default security assigned to generated results. Follow the same process as above, but this time select the "Access Incidents" object. In this example, we'll create two different groups: one will investigate results generated by financial controls, and the other will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



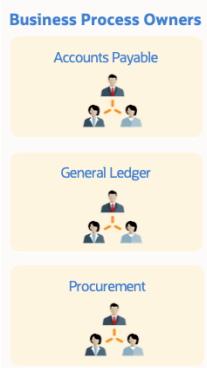


Deploy and Run Advanced Access Controls

Overview & Participants



The compliance/internal audit team works with business process owners to identify the initial risks to address. They deploy and run the corresponding controls and own the task of automating the delivery of quarterly SoD reports.



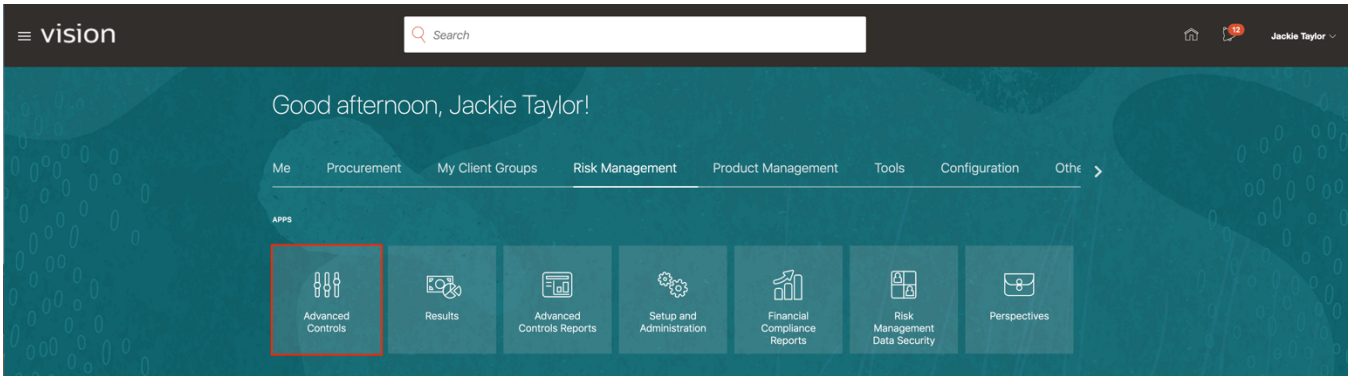
The business process owners work with the compliance team to identify the initial risks to address and will be involved in future identification of mitigating controls and remediation tasks related to reviewing conflicts and determining appropriate user access.

Step 1: Identify Risks

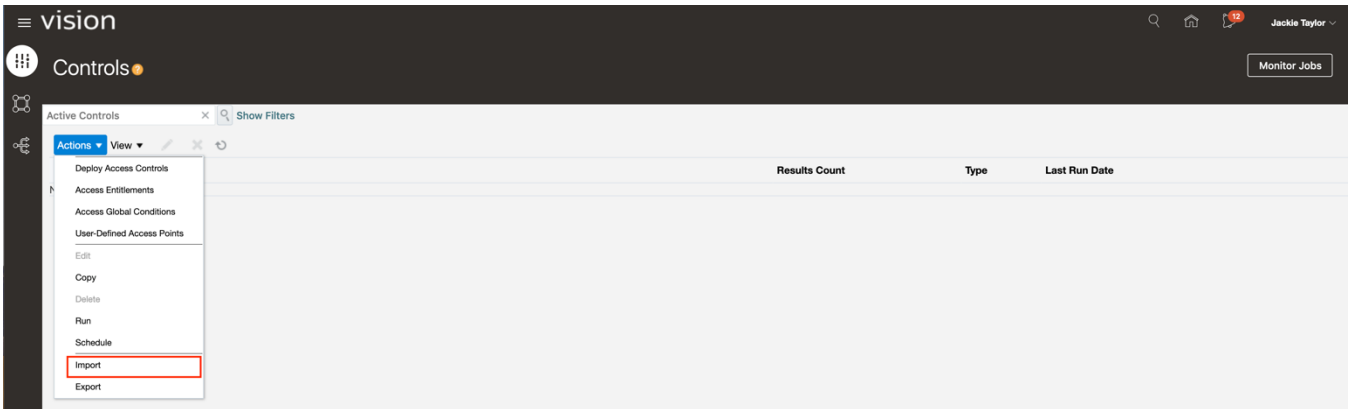
Start with your existing risks based on your interactions with auditors, and map them to our pre-built controls; or deploy the starter pack we provide, which is a subset of our pre-built control library. We've selected controls that are popular because they address risks of cash leaks and financial misstatements.

Step 2: Import Controls

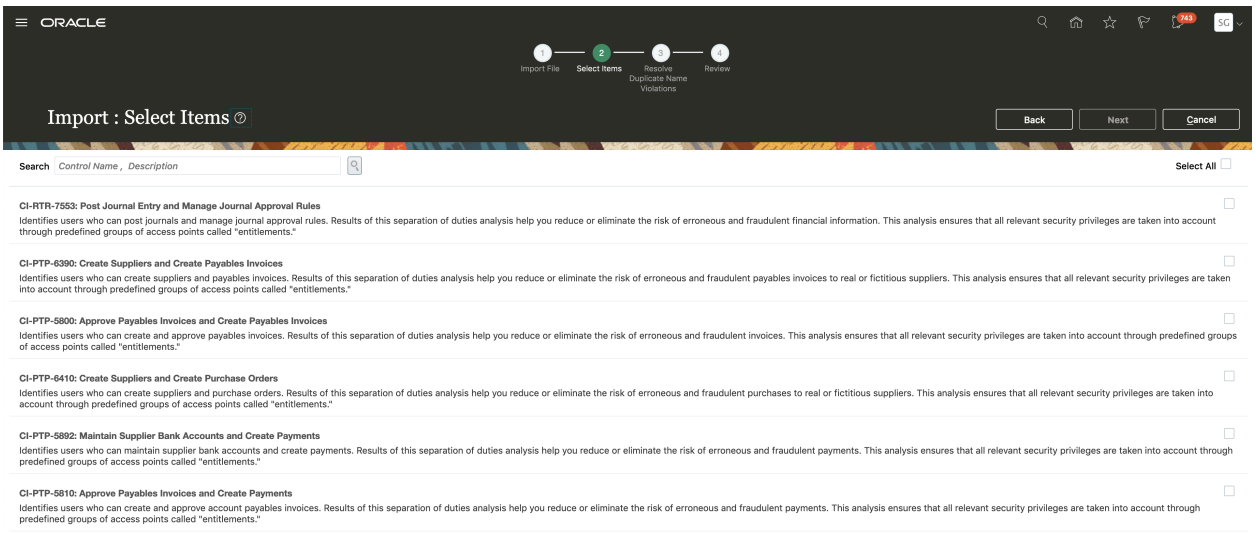
Navigate to Risk Management and click Advanced Controls:



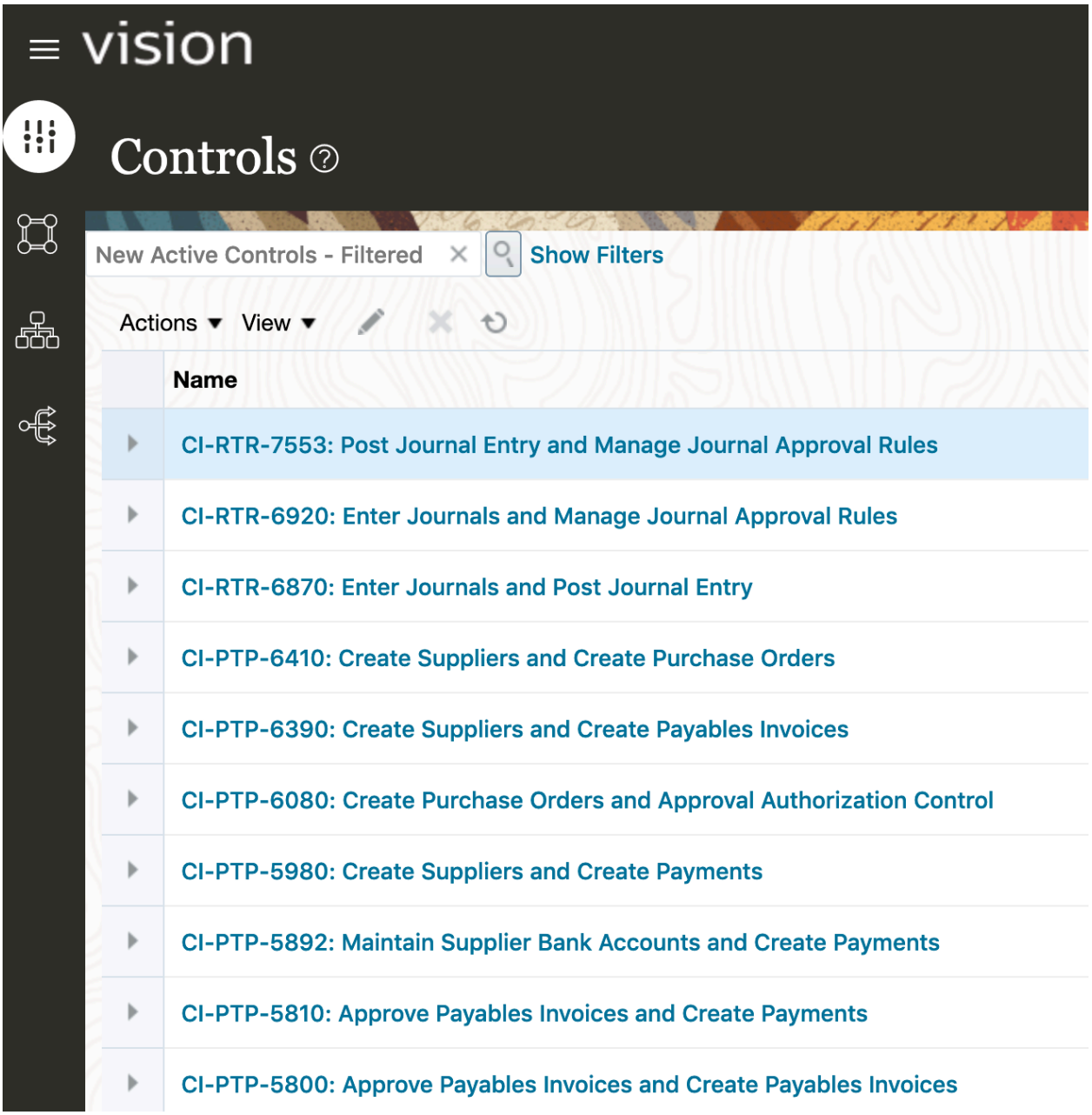
Select Actions > Import and select the 'Top 12 Advanced Access ERP Controls.xml' file: https://cloudcustomerconnect.oracle.com/posts/1aaf01117a



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.

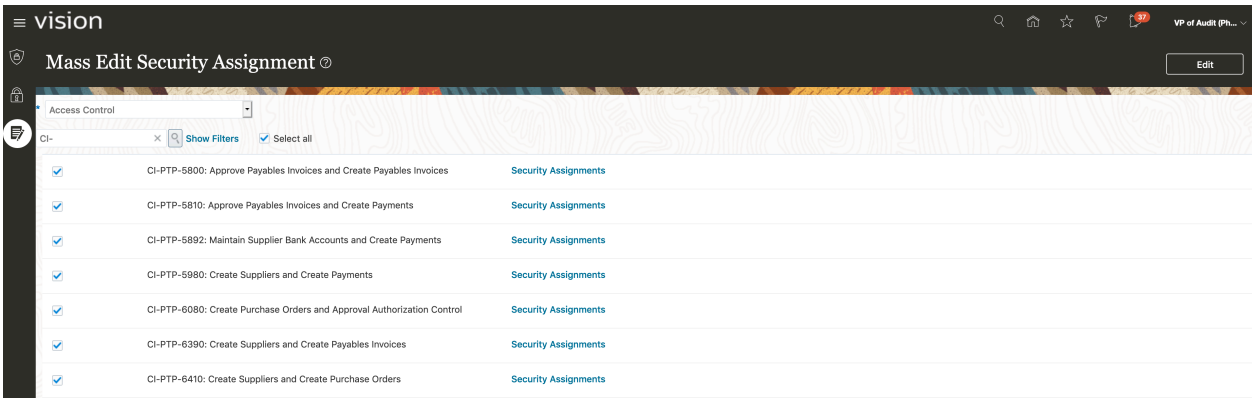


Since you are the one importing the controls, you automatically become their owner. Next you'll add an important user assignment group.

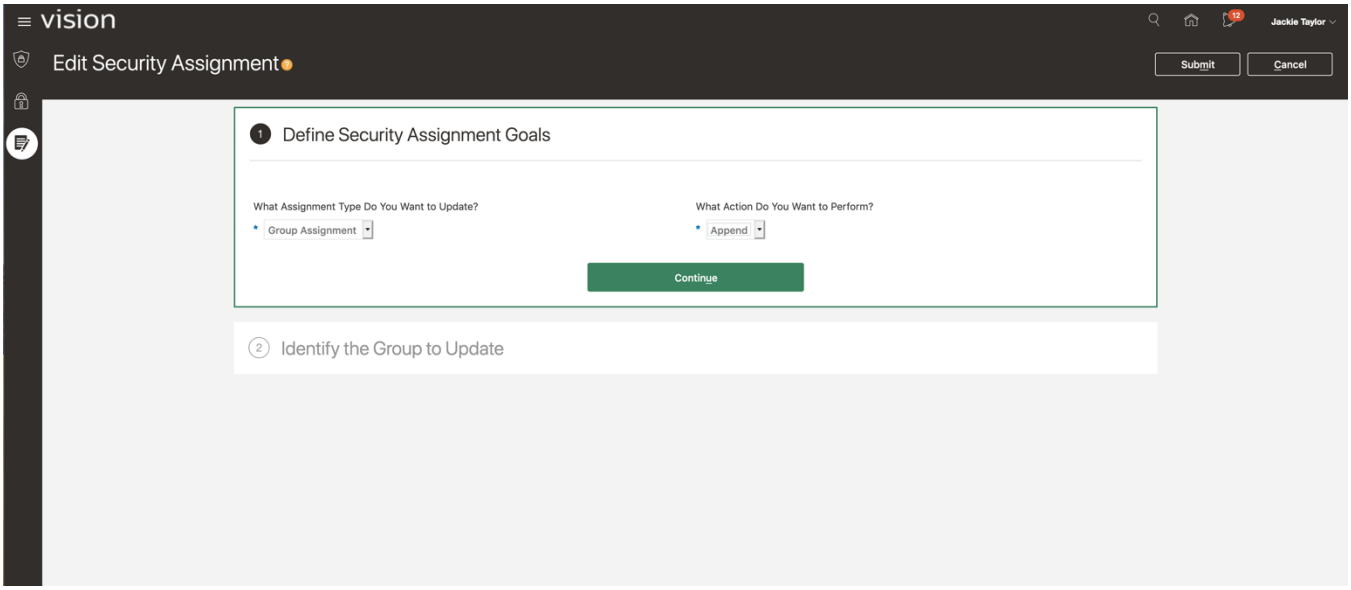
Step 3: Security Assignment – Control

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

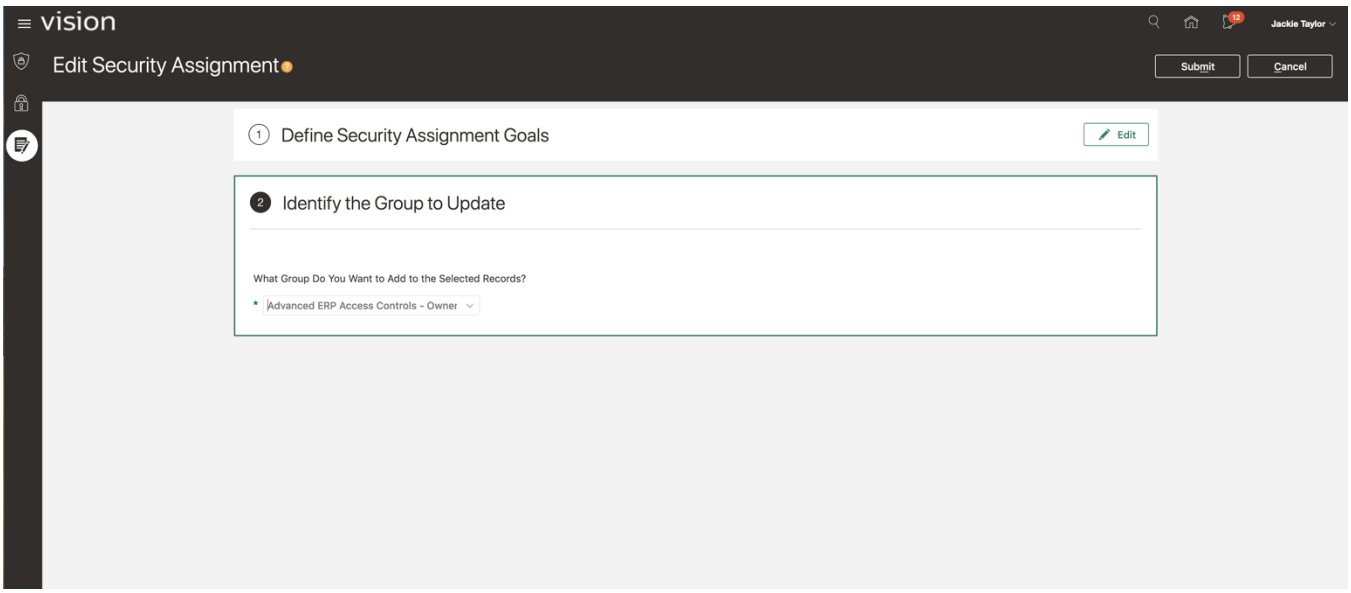
Tick the Select All check box, then click Edit:



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

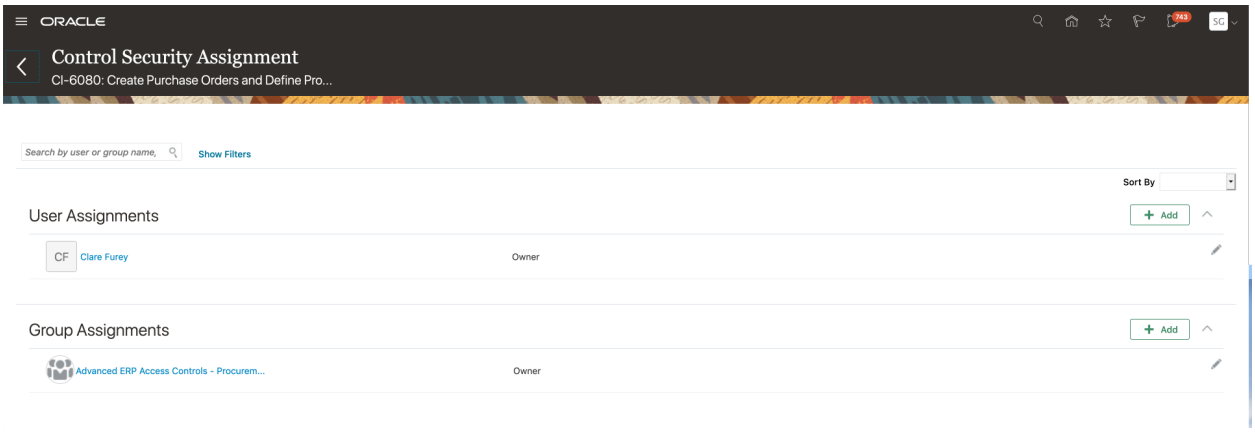


Select the group you created earlier: in this case, ‘Advanced ERP Access Controls – Owner,’ and click Submit:

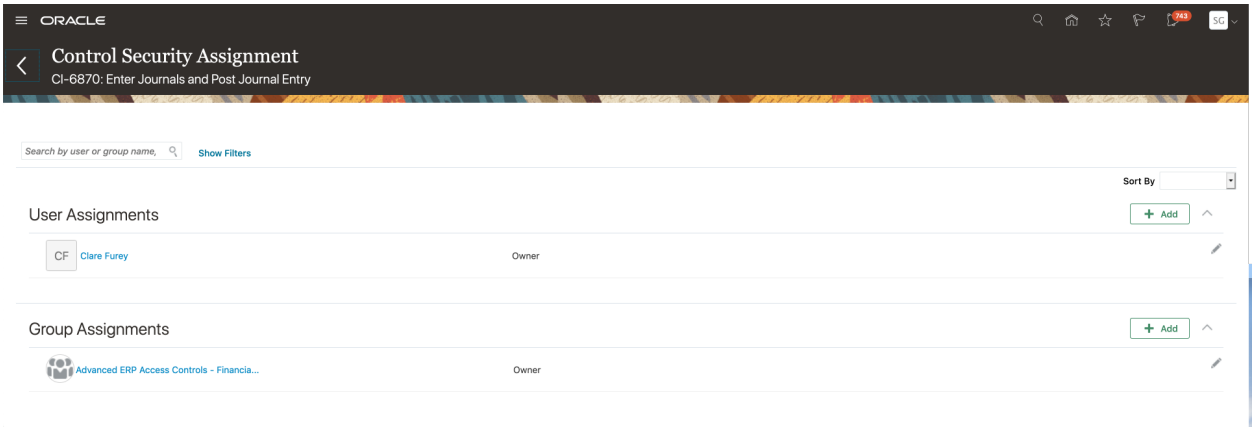


Step 4: Security Assignment – Control Result

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

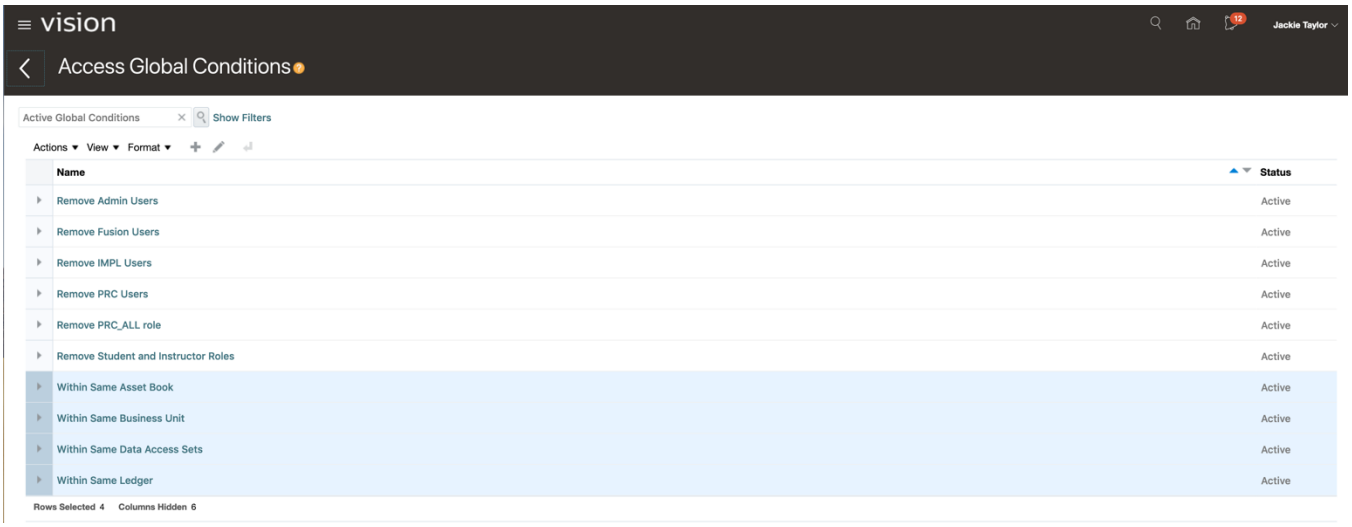
Navigate to Risk Management > Advanced Controls. Click on Actions > Access Global Conditions. Select Actions > Import and select the "Top 4 Global Conditions.xml" file: https://cloudcustomerconnect.oracle.com/posts/1aaf01117a

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.)

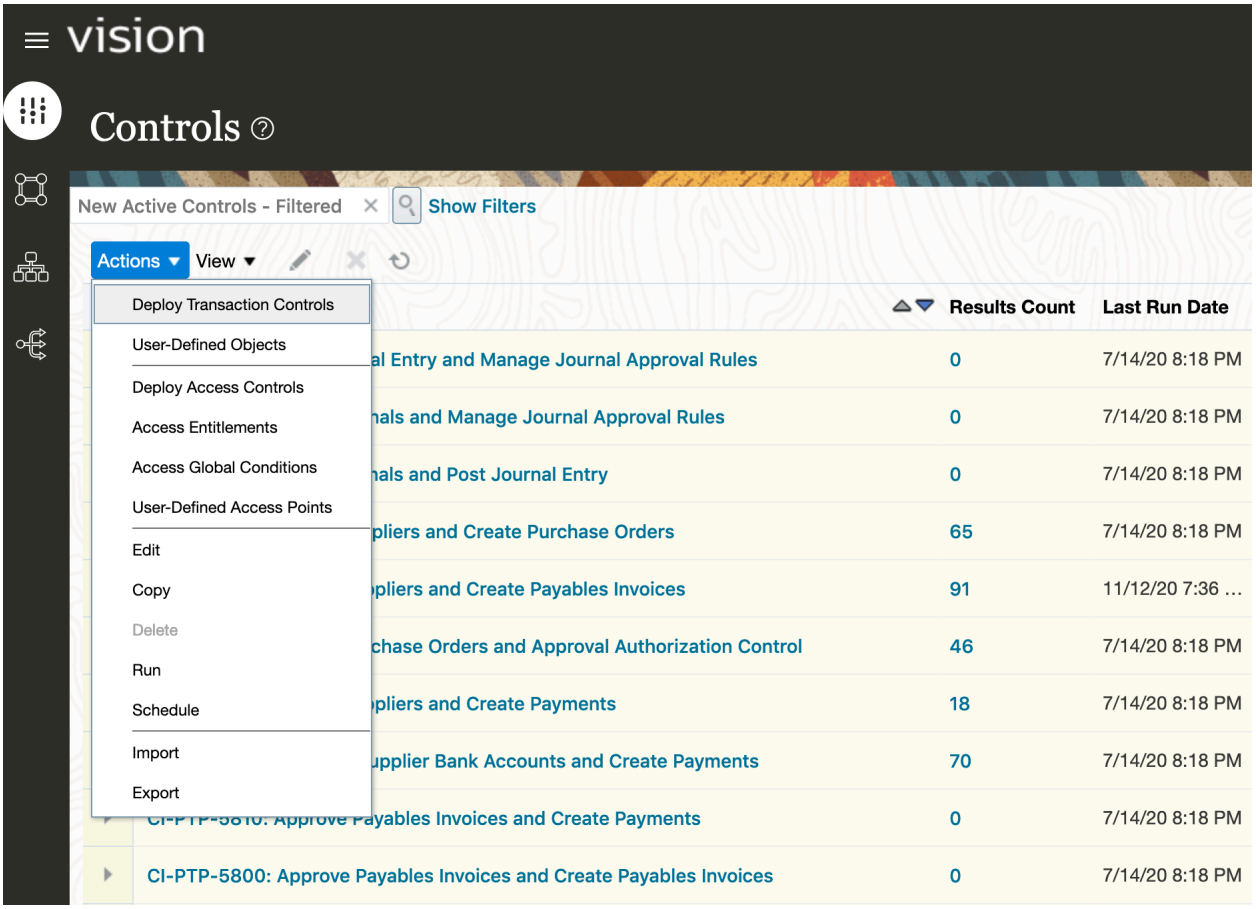
You may also consider adding additional global conditions to exclude known superusers or their roles, especially in a development environment.

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.

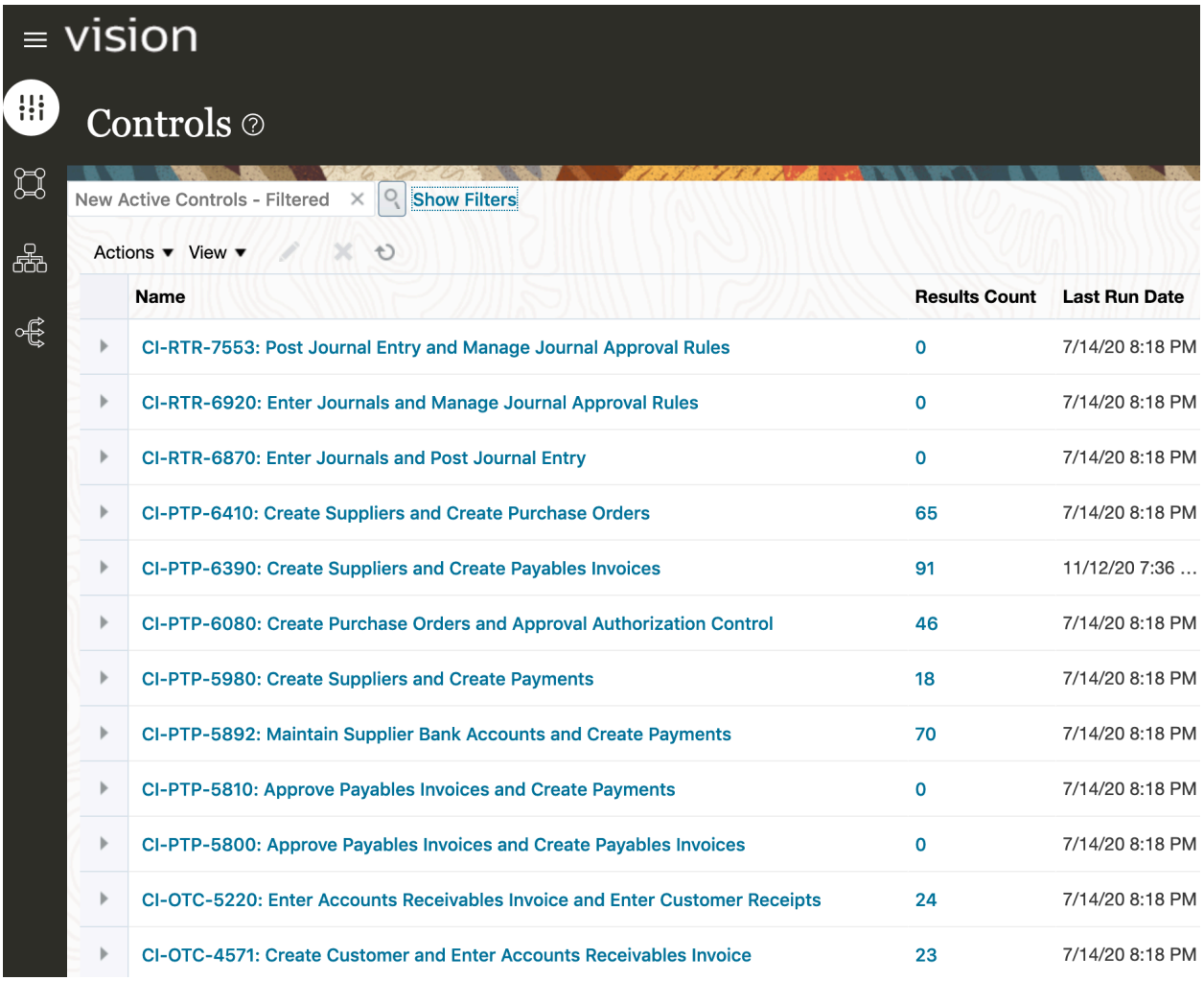


Step 6: Run Controls

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

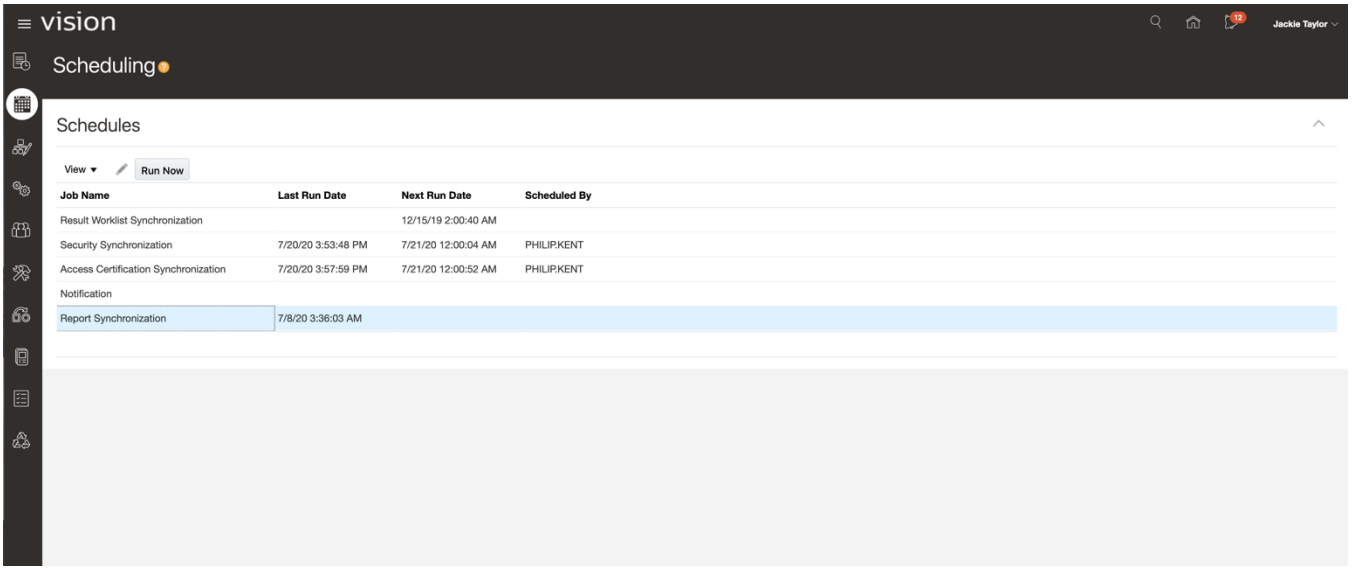


When control analyses have completed, the results counts are populated:


vision
Controls
New Active Controls - Filtered
Show Filters
Actions
View
Name
Results Count
Last Run Date
CI-RTR-7553: Post Journal Entry and Manage Journal Approval Rules
0
7/14/20 8:18 PM
CI-RTR-6920: Enter Journals and Manage Journal Approval Rules
0
7/14/20 8:18 PM
CI-RTR-6870: Enter Journals and Post Journal Entry
0
7/14/20 8:18 PM
CI-PTP-6410: Create Suppliers and Create Purchase Orders
65
7/14/20 8:18 PM
CI-PTP-6390: Create Suppliers and Create Payables Invoices
91
11/12/20 7:36 ...
CI-PTP-6080: Create Purchase Orders and Approval Authorization Control
46
7/14/20 8:18 PM
CI-PTP-5980: Create Suppliers and Create Payments
18
7/14/20 8:18 PM
CI-PTP-5892: Maintain Supplier Bank Accounts and Create Payments
70
7/14/20 8:18 PM
CI-PTP-5810: Approve Payables Invoices and Create Payments
0
7/14/20 8:18 PM
CI-PTP-5800: Approve Payables Invoices and Create Payables Invoices
0
7/14/20 8:18 PM
CI-OTC-5220: Enter Accounts Receivables Invoice and Enter Customer Receipts
24
7/14/20 8:18 PM
CI-OTC-4571: Create Customer and Enter Accounts Receivables Invoice
23
7/14/20 8:18 PM

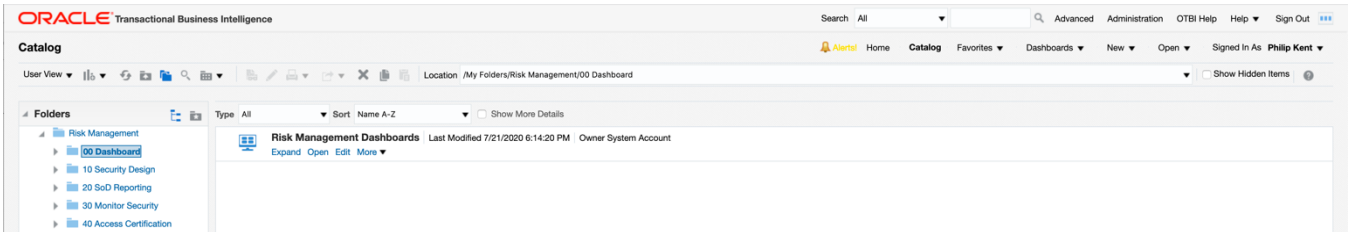
Step 7: Run Report Synchronization

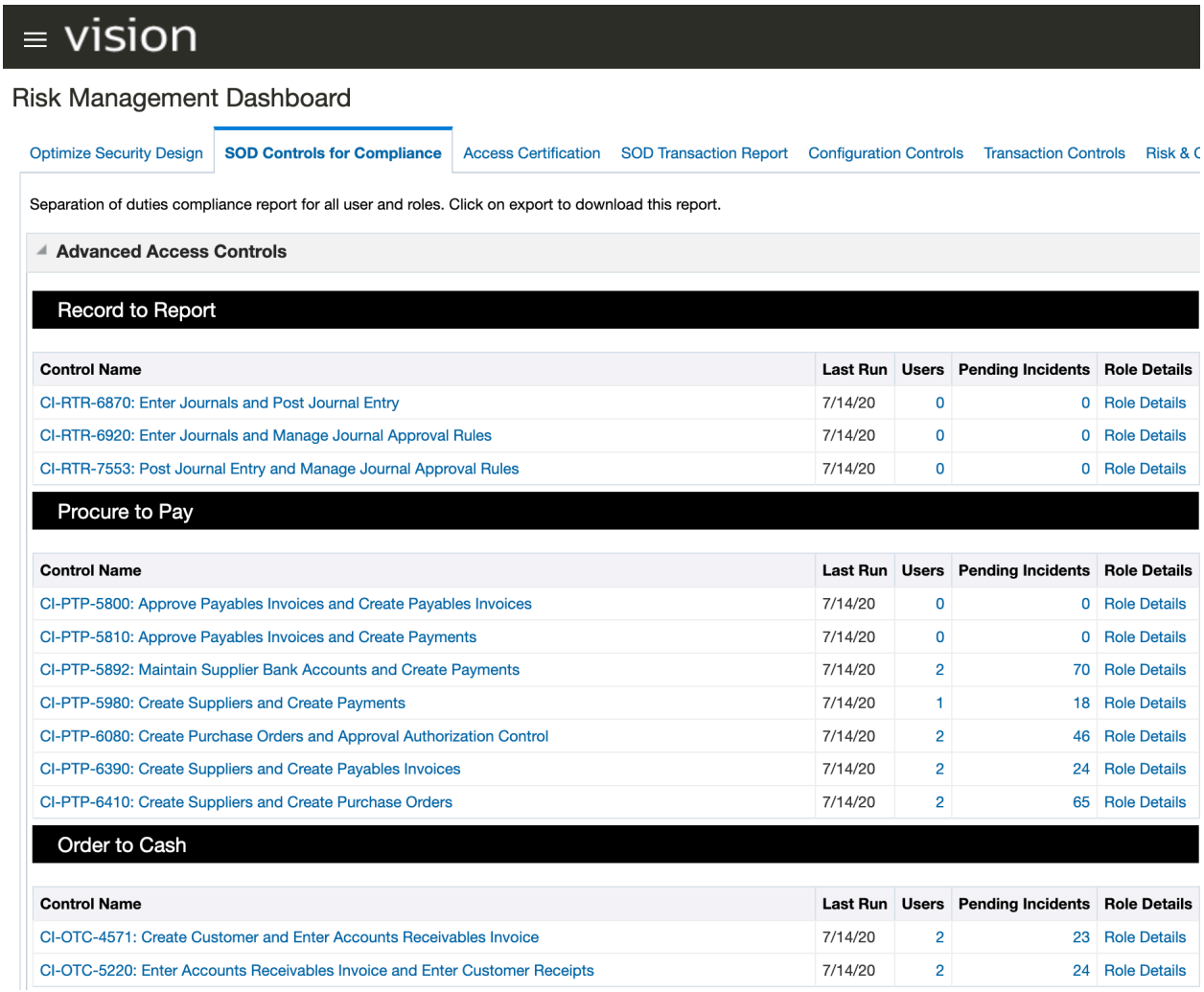
Navigate to Risk Management > Setup and Administration. Select the Scheduling tab, then run Report Synchronization:



Step 8: Review the Risk Management Dashboard

Navigate to the "00 Dashboard" and click on Open for the "Risk Management Dashboards." Click on the "SOD Compliance Report" tab:





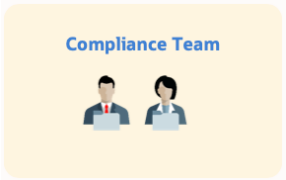
Check accuracy by comparing a few users and roles identified in Risk Management with those identified by your existing process.

MIGRATE TO PRODUCTION

Once you're comfortable with the steps you've taken in a non-production environment, perform the same steps in production, including the prerequisites.

ACCEPT INCIDENTS WITH MITIGATING CONTROLS

Overview & Participants

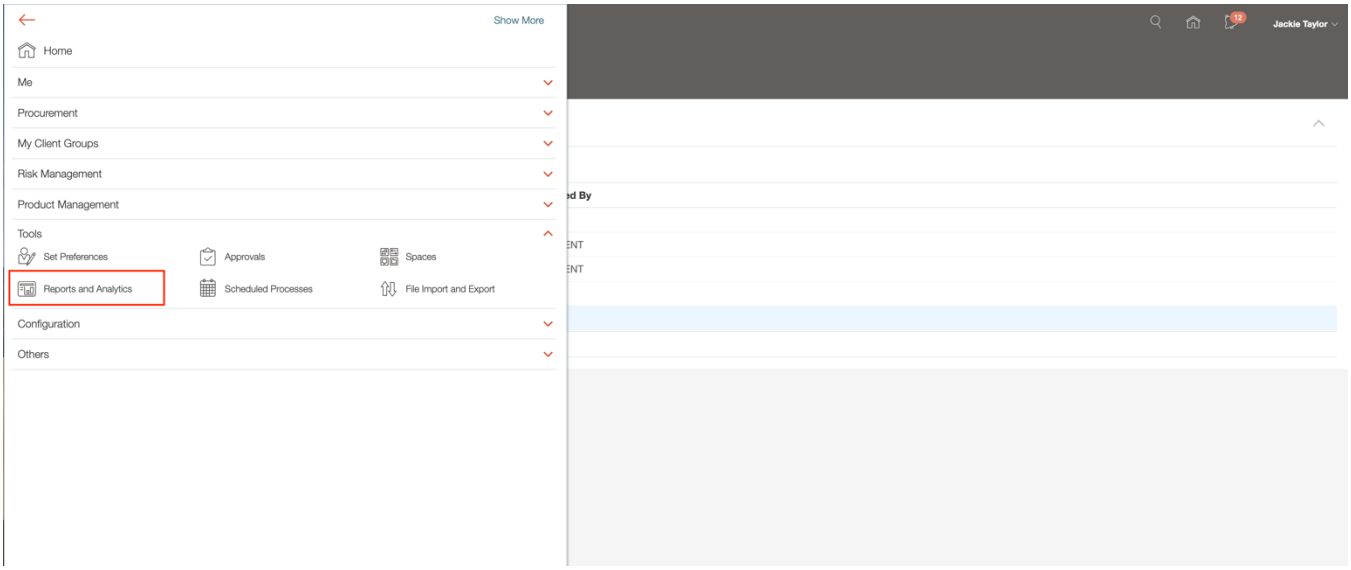


The compliance team accepts incidents with known mitigating controls, with the goal of reducing the number of pending incidents to zero.

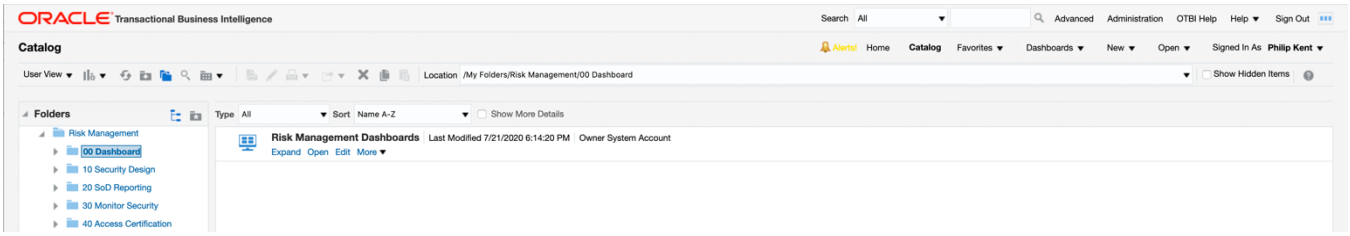
Since you've been using another process for SoD analysis and reporting, it's likely you've already identified mitigating controls for users with access violations. Now you'll accept these results and note the mitigating controls:

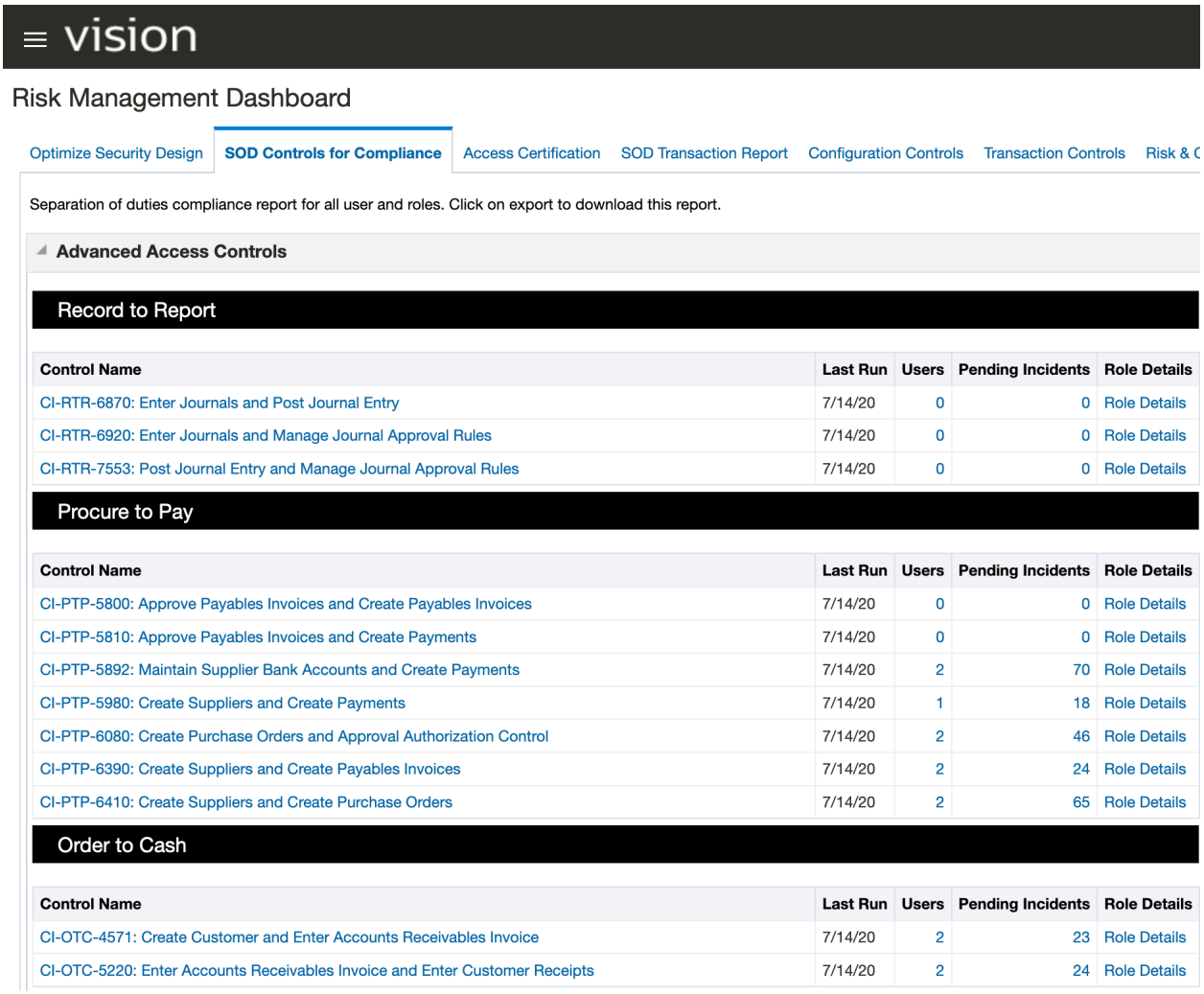
Step 1: Review Risk Management Dashboard

Navigate to Reports and Analytics and select Browse Catalog:



Navigate to Custom > Risk Management > 00 Dashboard, and click on Open for the "Risk Management Dashboards." Click on the "SOD Compliance Report" tab. Consider making this a favorite:

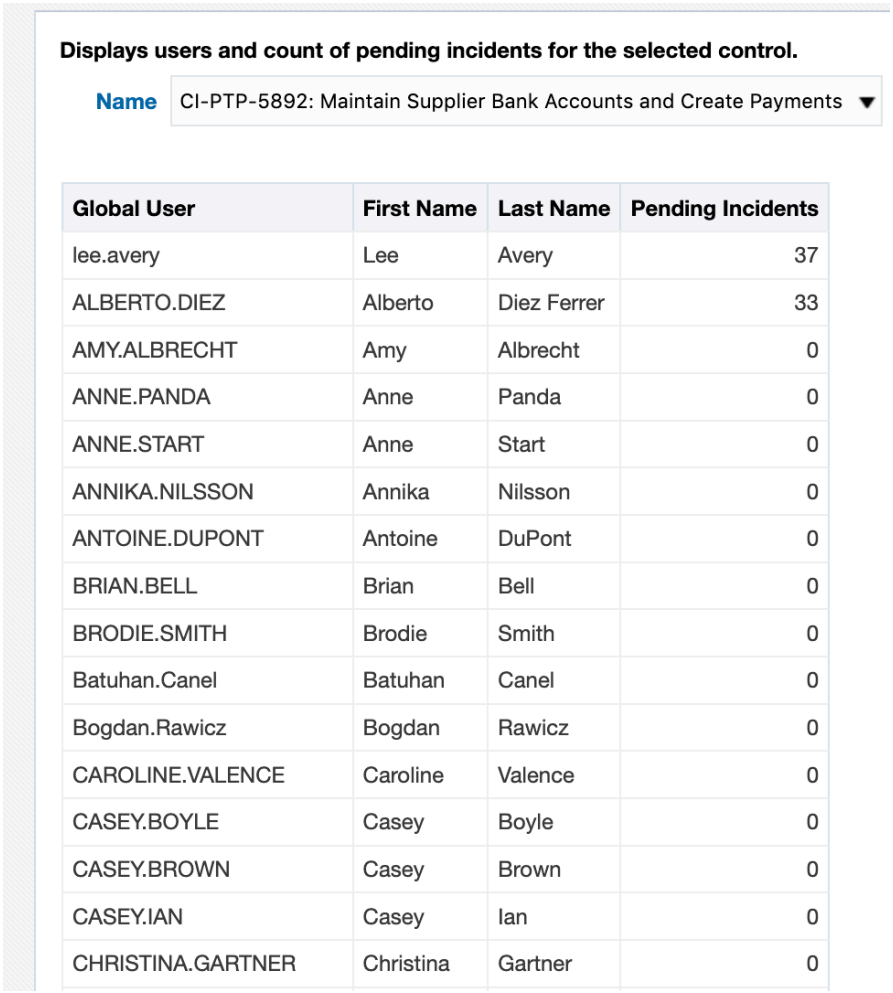




Step 2: Work through each control

We can reference users and roles that have violations for each control by clicking the ‘Users’ or ‘Role Details’ column value link, or directly begin accepting incidents and adding mitigating controls by clicking the pending incidents count.

Here’s an example of the information available when drilling on a user count:



Displays users and count of pending incidents for the selected control.

Name CI-PTP-5892: Maintain Supplier Bank Accounts and Create Payments

Global User	First Name	Last Name	Pending Incidents
lee.avery	Lee	Avery	37
ALBERTO.DIEZ	Alberto	Diez Ferrer	33
AMY.ALBRECHT	Amy	Albrecht	0
ANNE.PANDA	Anne	Panda	0
ANNE.START	Anne	Start	0
ANNIKA.NILSSON	Annika	Nilsson	0
ANTOINE.DUPONT	Antoine	DuPont	0
BRIAN.BELL	Brian	Bell	0
BRODIE.SMITH	Brodie	Smith	0
Batuhan.Canel	Batuhan	Canel	0
Bogdan.Rawicz	Bogdan	Rawicz	0
CAROLINE.VALENCE	Caroline	Valence	0
CASEY.BOYLE	Casey	Boyle	0
CASEY.BROWN	Casey	Brown	0
CASEY.IAN	Casey	Ian	0
CHRISTINA.GARTNER	Christina	Gartner	0

Here’s an example of the information available when drilling on the role details:

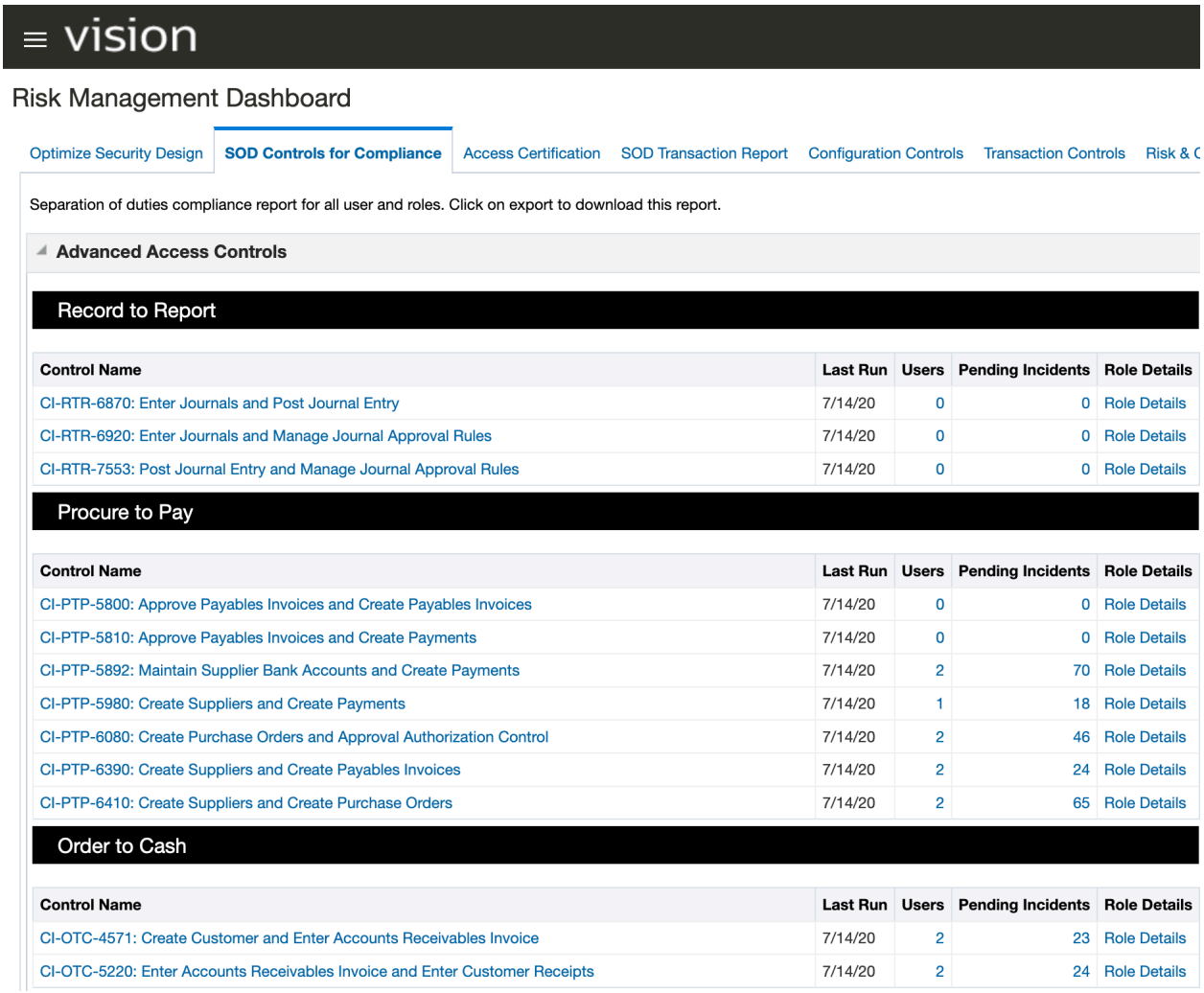
Displays roles and count of pending incidents for the selected control.

Name CI-PTP-5892: Maintain Supplier Bank Accounts and Create Payments

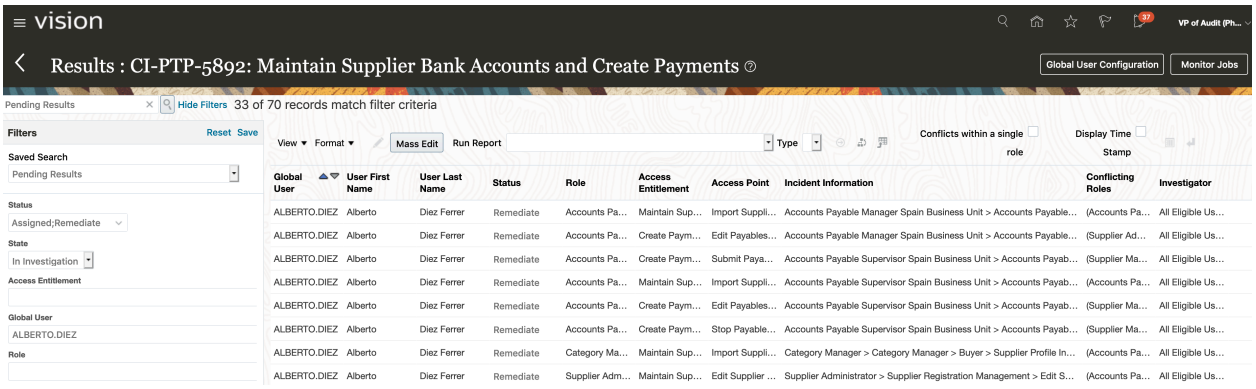
Role	Pending Incidents
Accounts Payable Supervisor	12
Accounts Payable Supervisor Spain Business Unit	12
Accounts Payable Manager	9
Accounts Payable Manager Spain Business Unit	9
Employee	8
Supplier Administrator	4
Financial Application Administrator	3
Buyer	2
Category Manager	2
Procurement Contract Administrator	2
Procurement Manager	2
Supplier Manager	2
Tax Manager	2
Accounts Payable Specialist Spain Business Unit	1
Accounts Payable Manager Australia Business Unit	0
Accounts Payable Manager Belgium Business Unit	0

Step 3: Accept incidents and add mitigating control

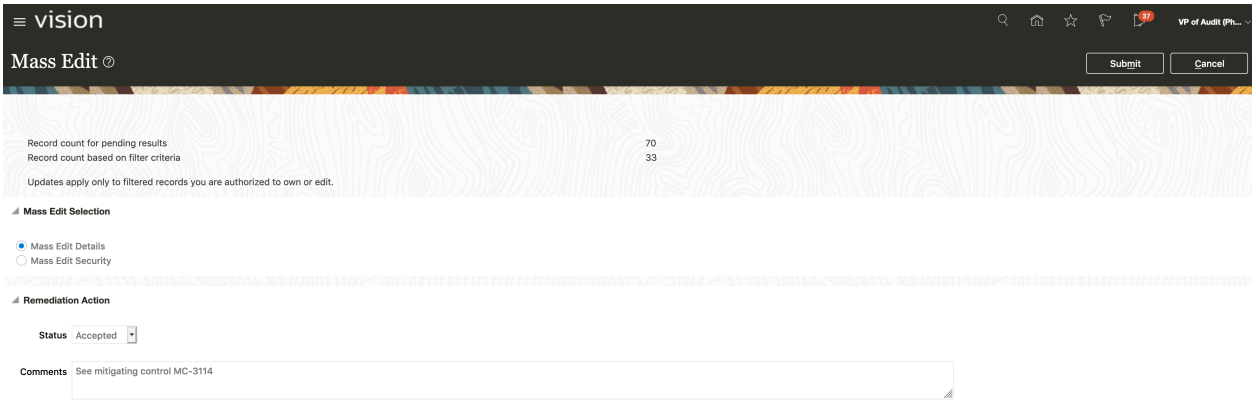
In this example, let's assume we want to accept incidents for control CI-PTP-5892: Maintain Supplier Bank Accounts and Create Payments for ALBERTO.DIEZ. Select the pending incidents count of 70:



Select Show Filters and in the Global User field, enter ALBERTO.DIEZ and click search:



Now click Mass Edit. Set status to Accepted and add the mitigating control reference to the comments, then submit:



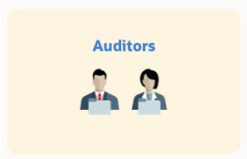
Iterate through this process.

Step 4: Refresh Dashboard

To see the updates reflected in the dashboard, run report synchronization.

DELIVER QUARTERLY REPORTS

Overview & Participants



Internal and external auditors reference the dashboard to verify expected controls exist, the last time they were run and pending incidents, and accepted incidents and their mitigating controls.

Stakeholders in the audit committee and C-suite also have the dashboard at their fingertips.

Step 1: Share the Dashboard

The dashboard you've been using to review conflicts and apply mitigating controls can be accessed by other interested stakeholders.

You can create new security assignment groups with view-only authorization (if there is no need for these stakeholders to edit or assign security), and/or you can add additional members to the groups you've already created.

FUTURE CONSIDERATIONS

Now that you've automated SoD and compliance reporting, you can consider expanding the scope to include more controls. The ultimate goal is to employ a continuous monitoring strategy where conflict violations are identified and remediated immediately, and SoD reporting is delivered to the right people at the right time.

Assuming a continuous monitoring strategy, consider scheduling the following jobs, in the following order, to run on a daily basis:

- Import User and Role Application Security Data Process
- Security Synchronization
- Global User Synchronization
- Control Analysis (select all controls to run in a batch)
- Report Synchronization

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

BEST PRACTICE CONTROL LIBRARY

There are over 130 ERP SoD and sensitive access controls to choose from. This step by step document considers 12 critical controls that span 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