ORACLE

Continuously Monitor Transactions

Step-by-step guide to finding and addressing unwanted Cloud ERP transactions

February 2021

SUMMARY

Oracle Risk Management Cloud lets you monitor Cloud ERP transactions, either as a primary or mitigating control. This document provides a guided process for configuring, testing and verifying some key controls. Risk Management's advanced analytics help raise visibility unexpected transactions that might otherwise go undetected.

This document provides step-by-step instructions to:

- Quickly deploy these key controls from our pre-built library of best-practice controls:
  - Procurement
    - 30001: Duplicate Payables Invoices
    - 30003: Backdated Purchase Orders
    - 40001: Supplier and Payables Invoices Created by the Same User
    - 40004: Payment Process Request Created by Same User Managing Suppliers
    - 40005: Suppliers and Purchase Orders Managed by the Same User
  - Financial Management
    - 32002: Manual Journals Posted After Period Close Date
    - 40006: Customers and Receivables Invoices Managed by the Same User
  - Self-Service Financials
    - 31004: Duplicate Expenses Submitted by Employee for Reimbursement
  - Supply Chain & Manufacturing
    - 40003: Item and Inventory Transaction Created by the Same User
- Continuously monitor changes to detect any fraudulent activities
- Investigate changes using dashboard reports

DEVELOP MODELS & CONTROLS IN A NON-PRODUCTION ENVIRONMENT

Initial Considerations

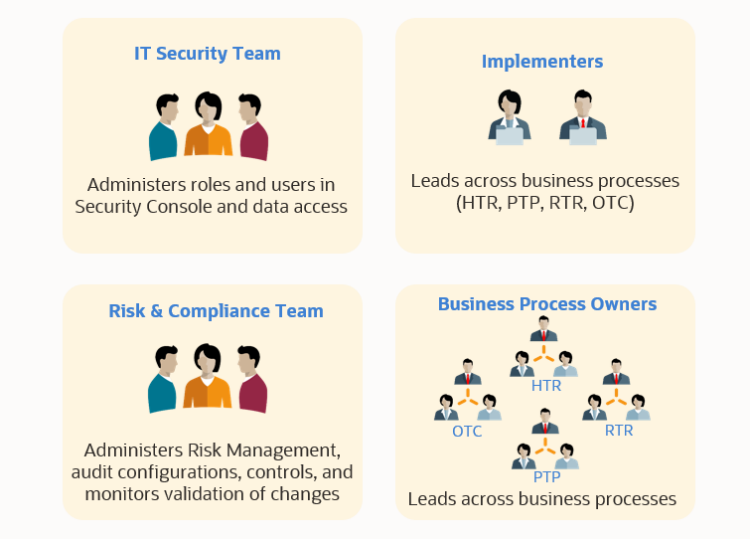
The initial step in any implementation is to describe what you want to end up with. In this case, it first means figuring out who is using Cloud ERP, how they interact with it, and what transactions will be monitored. For example, are they business process owners who are responsible for transactions, or perhaps internal auditors who must make sure that unexpected transactions are not created?

As you follow the steps in this guide, be sure to first review related documentation on Cloud ERP, securing and implementing Risk Management, and using Advanced Controls, which are referenced in this document's Related Resources section. Those guides will also help you to consider how predefined job roles are organized around functional processes and stakeholder groups, and how they might be customized to grant the most efficient and secure access.

In conjunction, it will help you define and secure participant responsibilities across your organization. Consider the answers to the following questions, which identify participants, responsibilities, user groups, and their security access:

- Who will determine what transactions to track?
- Who has access to create and approve the transactions?
- Who will monitor and audit the transactions?
- Who can be included in the review of transactions and provide supporting documentation?
- Who will determine remediation actions if needed?
- Who can take action on preventing the same transactions in the future?

For purposes of this this step-by-step guide to configure and implement controls for change tracking, the following stakeholders will participate in the process:



Risk Management Setup

Overview and Participants

Your application implementation team will enable Risk Management offering and run various jobs.

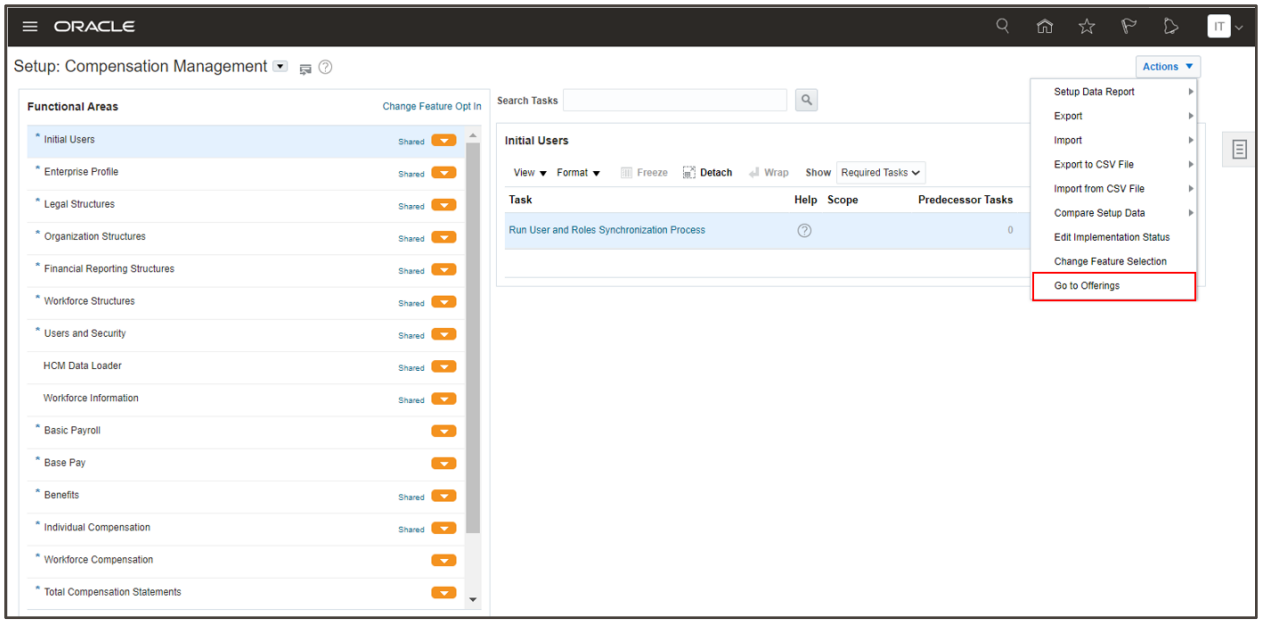
Your security team will grant access to the risk and compliance team to setup Risk Management.

Your risk and compliance administrator will setup Risk Management to support transaction controls and run various jobs.

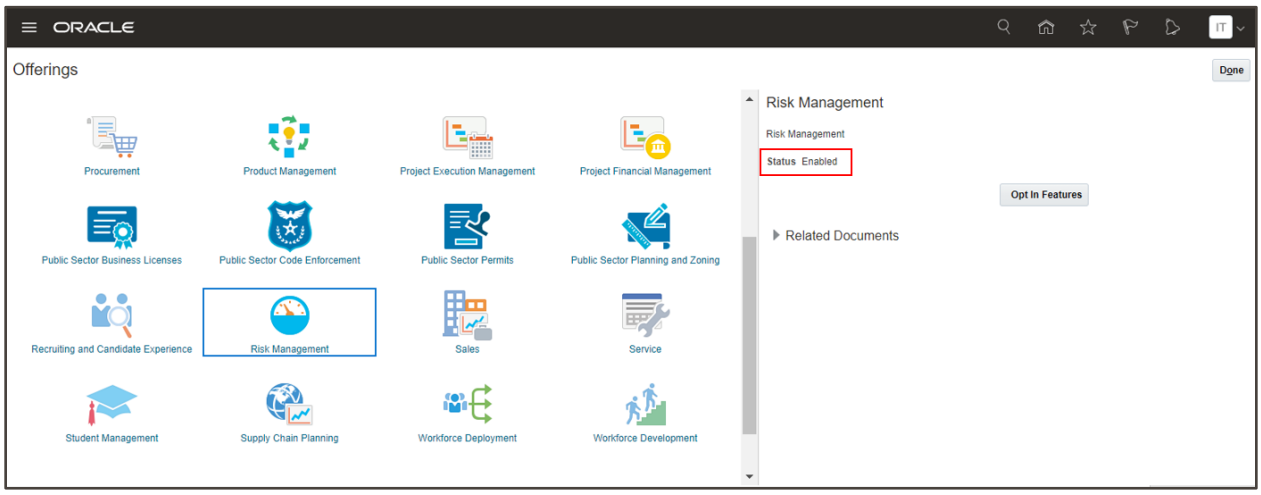
Step 1: Activate Risk Management

Your first step is to make sure Risk Management is activated in your test or development instance. Ask your system administrator or implementer to navigate to Setup and Maintenance.

Then, navigate to Actions > Go to Offerings.



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



Step 2: Assign Risk Management Job Roles

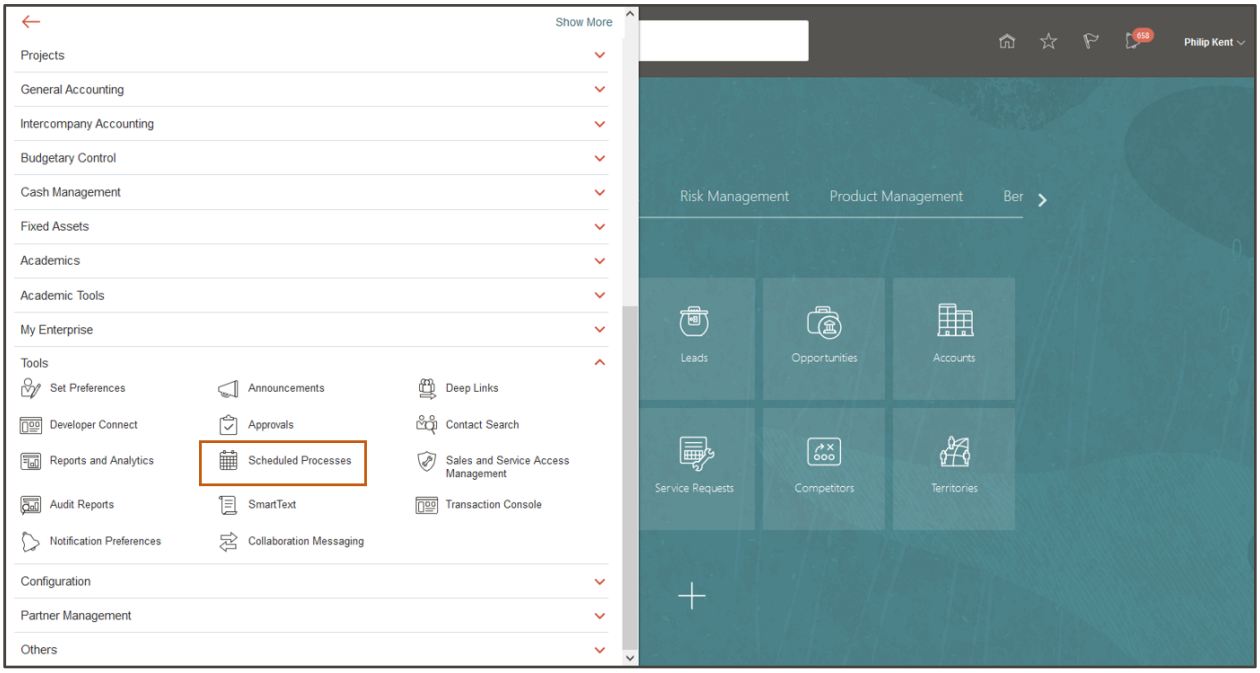
The security team grants user role access through the Security Console. Assign your user security to match their responsibility, whether it is to setup Risk Management, manage audit policies, or monitor transaction controls. Depending upon their participation across the processes documented, these members can be assigned one of the following predefined job roles:

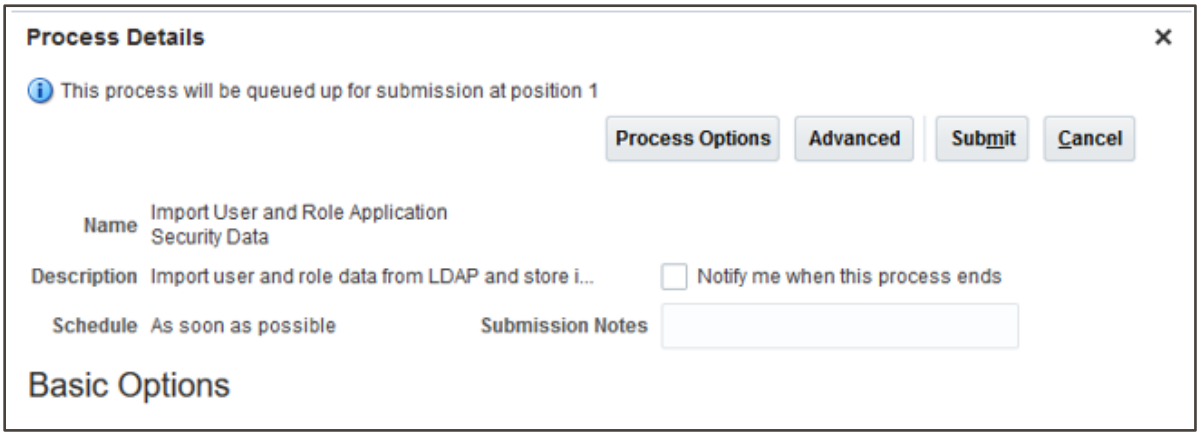
- Risk Administrator
    - Defines business object security, configures performance dates for data synchronization, runs jobs for controls, security, report and data synchronization, and related scheduling.
    - Role code: ORA_GTG_RISK_ADMINISTRATOR_JOB
- Application Implementation Consultant
    - Manages transaction controls, and includes BI Administrator role to maintain reports and dashboards between test, development, and production environments.
    - Role code: ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB
- Advanced Transaction Controls Analyst
    - Imports models, deploys controls, maintains reports, and investigates incident results for possible fraud.
    - Role code: ORA_GTG_APPLICATION_CONTROL_MANAGER_JOB
- IT Security Manager
    - Grants access to Security Console for administering roles and user access.
    - Role code: ORA_FND_IT_SECURITY_MANAGER_JOB

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

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 user security is current, navigate to the Scheduled Processes work area. Select Schedule New Process, search and Submit the 'Import User and Role Application Security Data' process. You might need someone with IT Security Manager access to help you.

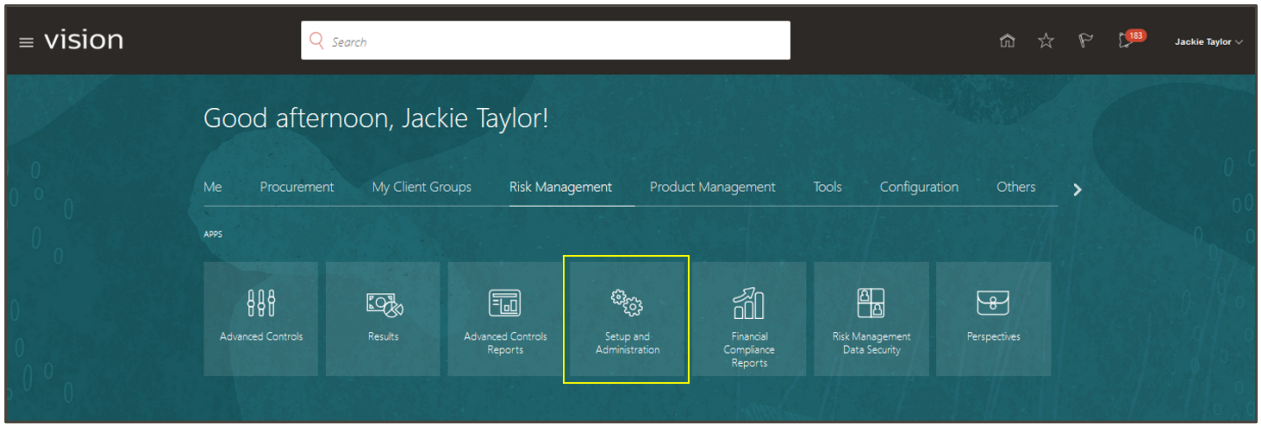




If you need to setup this job on a regular schedule, select the 'Advanced' button instead of Submit to define the schedule.

Step 4: Configure Advanced Controls

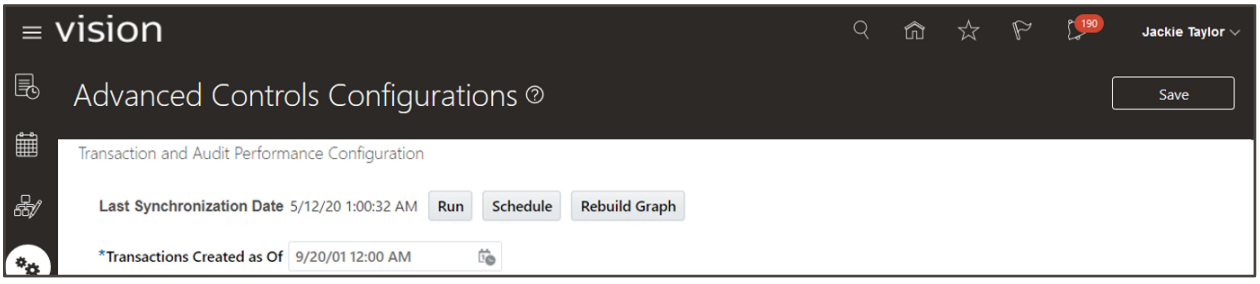
As a risk and compliance administrator, you will define a created as-of date as the starting point find transactions. Begin by navigating to Risk Management > Setup and Administration.



Next, click the tab for Advanced Controls Configuration. For the 'Transaction and Audit Performance Configuration' region, you need to set a date for Transactions Created as Of. Before setting the date, consider the following:

- The timeframe that business owners and auditors want to evaluate. (You can use different dates in development vs production environments.) A more recent date yields faster analyses, so we suggest starting with a very recent date to accelerate your initial explorations - e.g., three months ago – then revising the date once you are satisfied with your analyses. A typical implementation will settle on one year, then consider updating that annually - see "Ongoing Use" below.
- Consider the frequency at which you will run transaction controls. For example, transactions are captured when created, updated and approved, which might occur across several months.

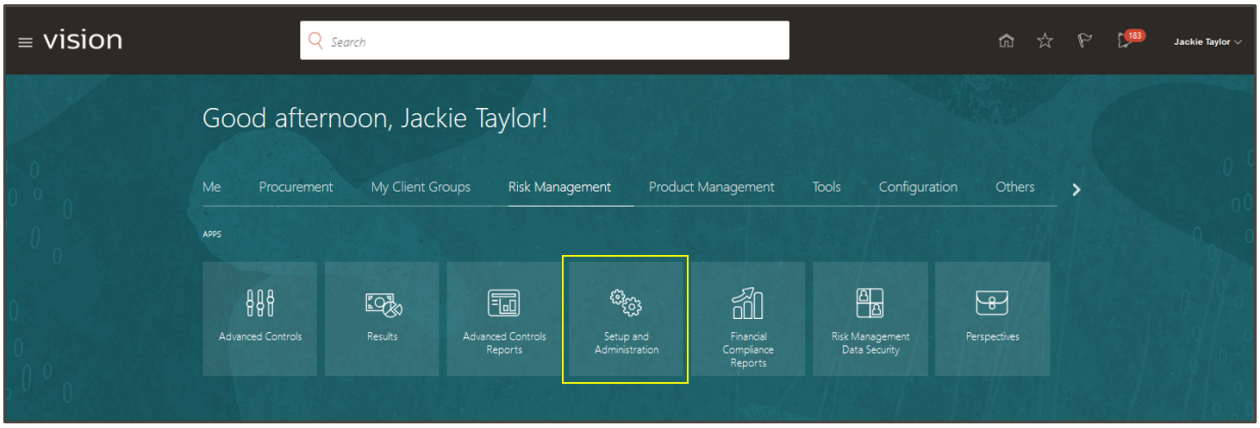
Save the page. No other action is required on the page at this time.



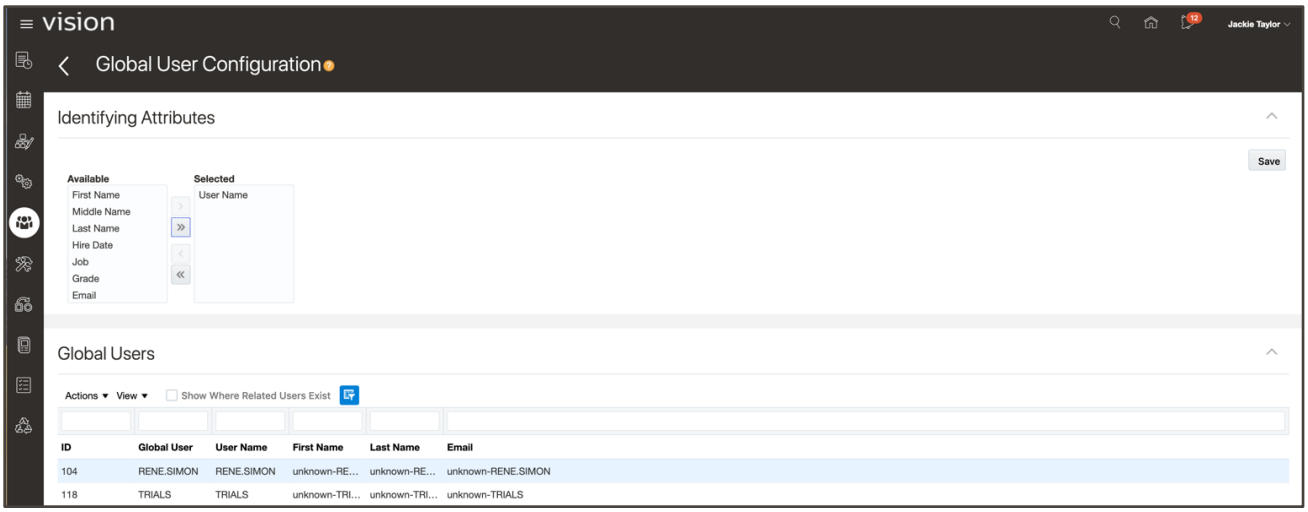
***Note**: Wait to select 'Run' for synchronization until you have imported delivered library content. Synchronization only applies to business objects (BOs) used in a model or control. If it is not used, it will not be synchronized.*

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

Global user information is used across advanced controls and needs to be run for transaction controls. Navigate to Risk Management and click Setup and Administration.



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

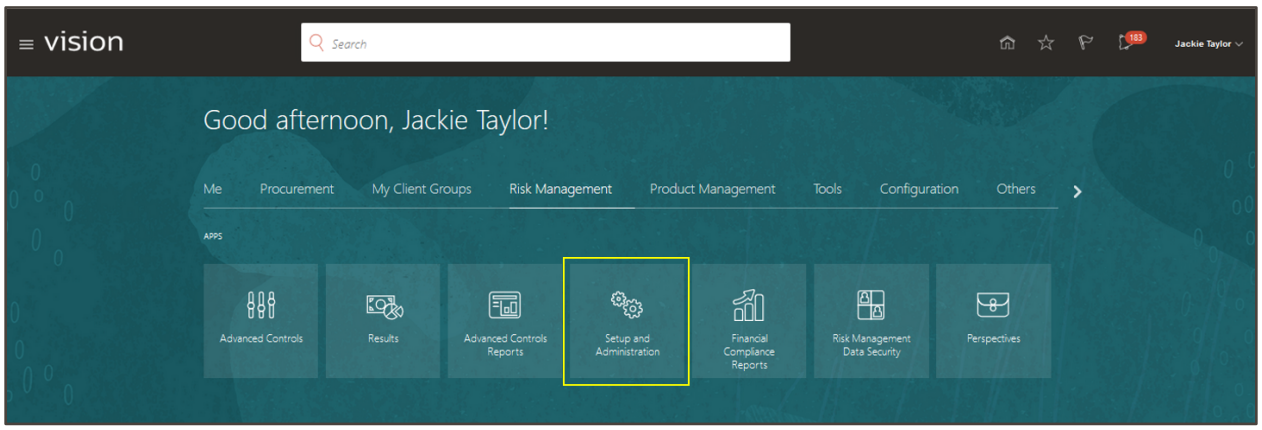


Once that job completes, the Global Users section is populated. These are users synchronized from the Users area in Security Console. The job role assignments for these users will be evaluated if using access control analysis and the global user name is the value associated to incidents identified.

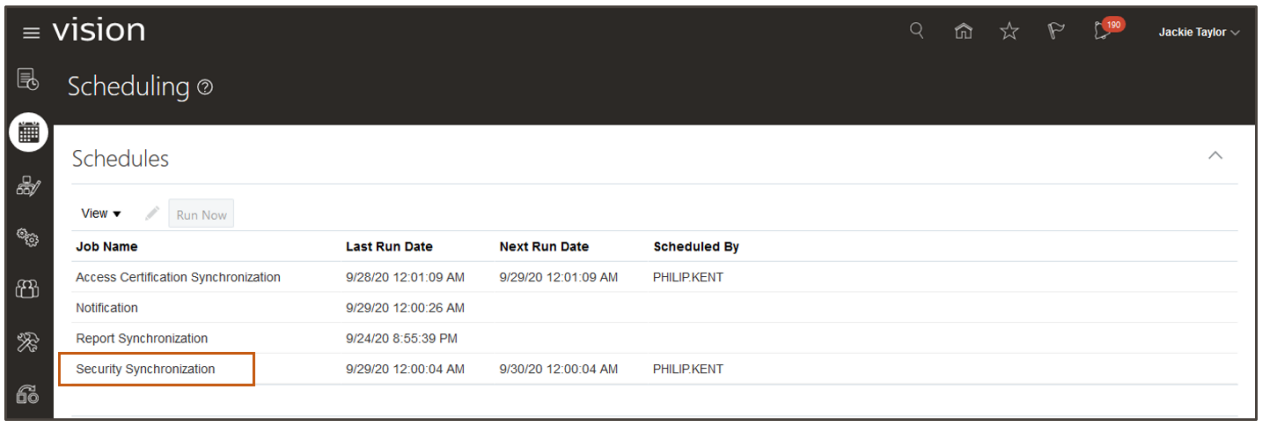
Step 6: Run the Security Synchronization Job

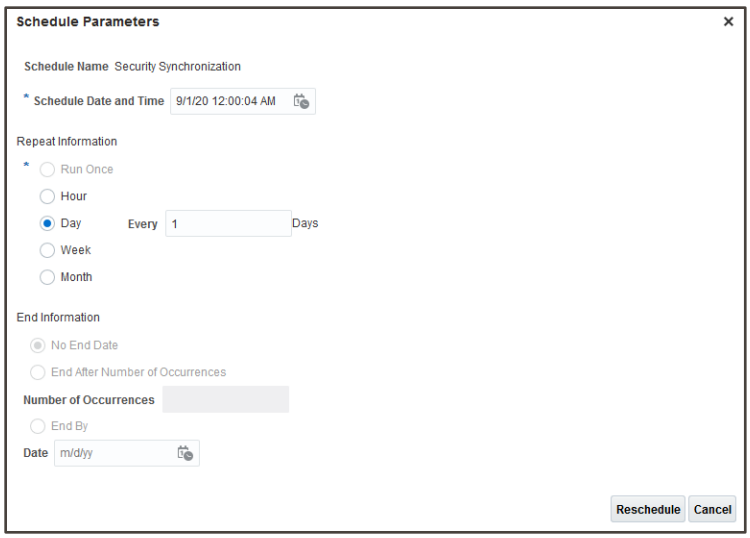
Anytime there are changes made in Security Console, be sure to run the Security Synchronization job, which updates who can access what in Risk Management. The job should be scheduled to run at least daily.

Navigate to Risk Management > Setup and Administration.



Go to the Scheduling tab and select 'Security Synchronization' job. Click 'Run Now' option to run immediately. To setup or change the job's schedule, click the Edit icon in toolbar.



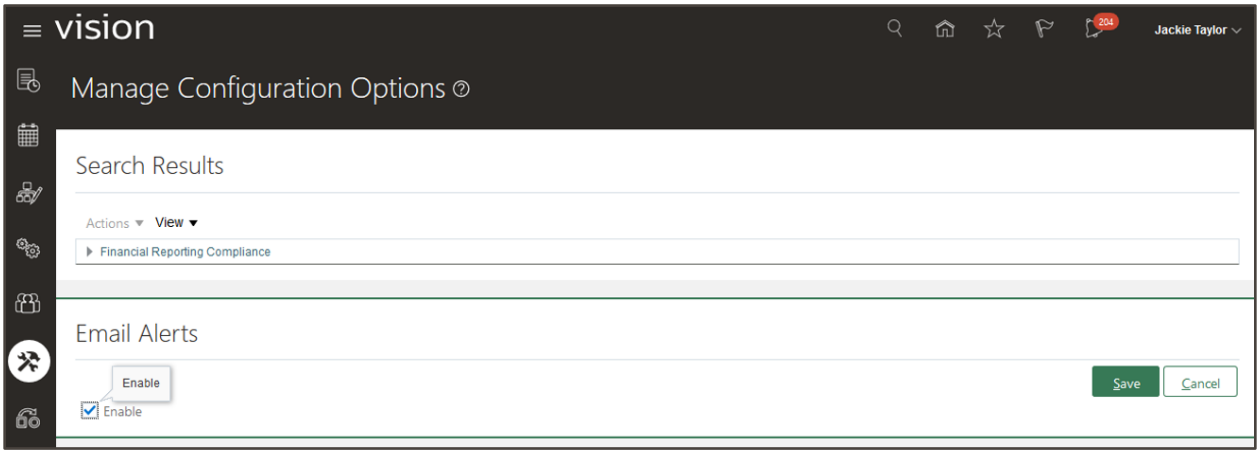

Schedule Parameters
Schedule Name Security Synchronization
* Schedule Date and Time 9/1/20 12:00:04 AM
Repeat Information
* Run Once
Hour
Day Every 1 Days
Week
Month
End Information
No End Date
End After Number of Occurrences
Number of Occurrences
End By
Date m/d/yy
Reschedule
Cancel

Step 7: Enable Email Alerts (Optional)

You can turn on a global setting in Risk Management to send email messages to users when worklists or tasks require their attention. The option only enables email alerts, but users will still get a bell notification of the task. Advanced control notifications include investigators of incident results, and creation or edit of the controls.

To enable email, navigate to Setup and Administration > Manage Configuration Options tab. Select Edit in the Email Alerts region.

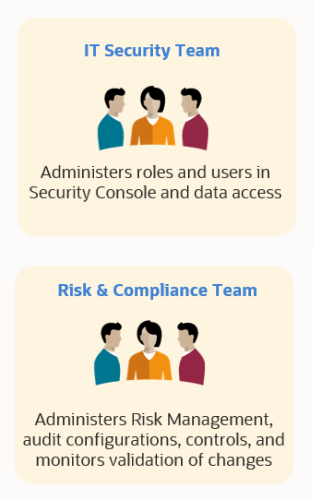
Select the Enable check box, and click Save.



Note: Evaluate if or when this email option is set in your development environment. Keep in mind there may be other Risk Management activities and test users that will be impacted.

Risk Management Data Security

Overview and Participants



Your security team will enable data security access by business object and/or product area to the risk and compliance team.

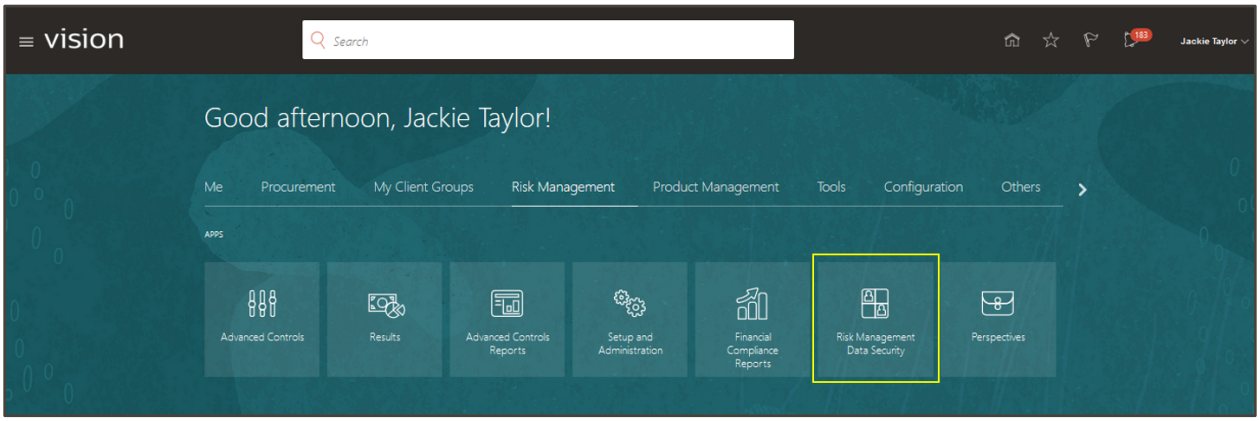
Your risk and compliance administrator will run and create job scheduling in Risk Management to support transaction controls, and maintain related user groups by area.

Step 1: Assign Business Object Security

As part of creating and managing models and controls in Advanced Controls, users need to be granted data access in Risk Management to business objects. For example, your organization may define an internal audit group to configure transaction policies, but the security team will need to grant data access that functionally aligns to those who will manage transaction models and controls by business area.

There are two ways to define data security in Risk Management: by functional area (such as Models) or specific business objects (like Supplier). Once you have one or more users setup with business object security, you can leverage their settings and copy it for other users.

To configure business object security, navigate to Risk Management > Risk Management Data Security work area.

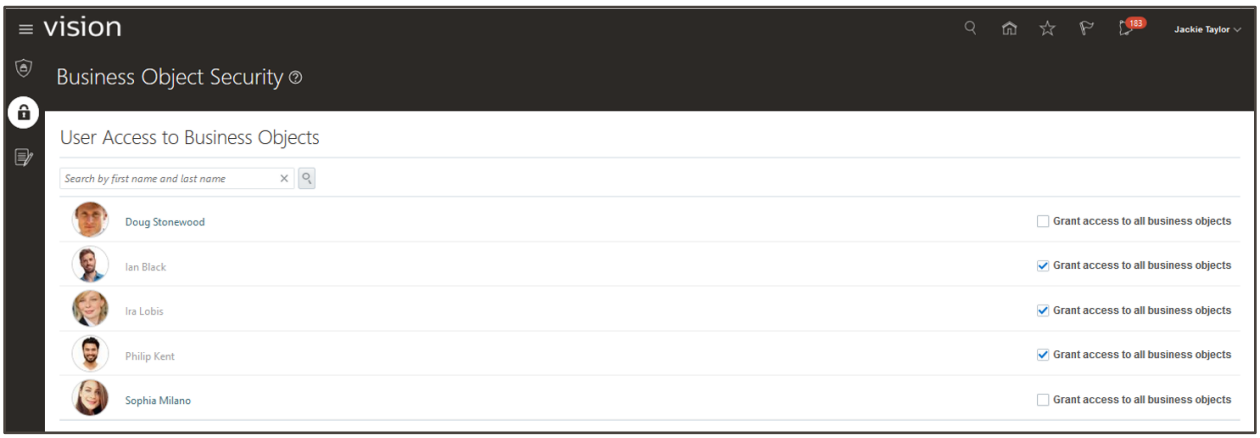


Select the Business Object Security tab.

Users available to assign business object (data) security are those who have been granted the 'Advanced Transaction Controls Analyst' job role, or a custom role that includes access to related duty roles for models and/or controls.

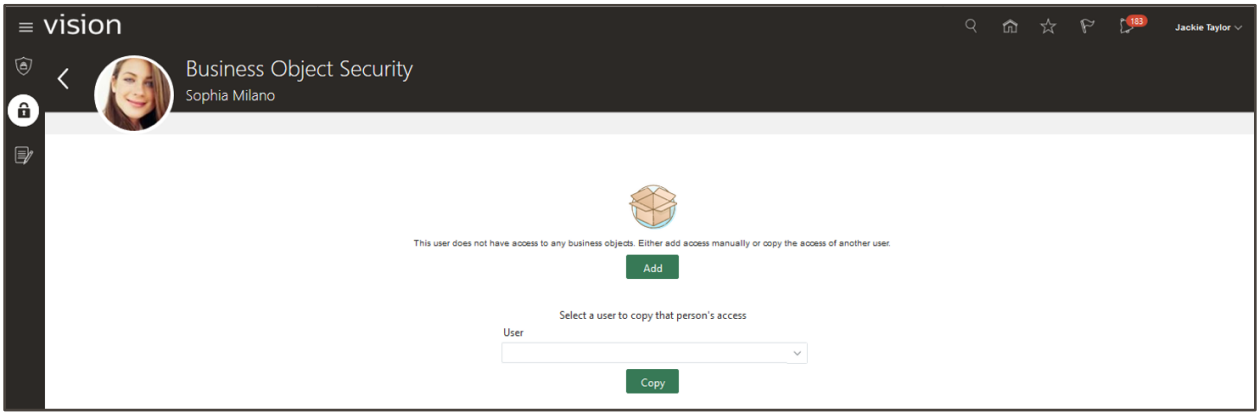
Note: Control incident result access is not dependent on this business object data security, only models and controls.

Here in the development environment, you might grant one user access to all business objects, by selecting the 'Grant access to all business objects' check box. However, in this first example, we will define user's access based on their business process or functional area of responsibility. Use the search dialog to find and select the user's name.

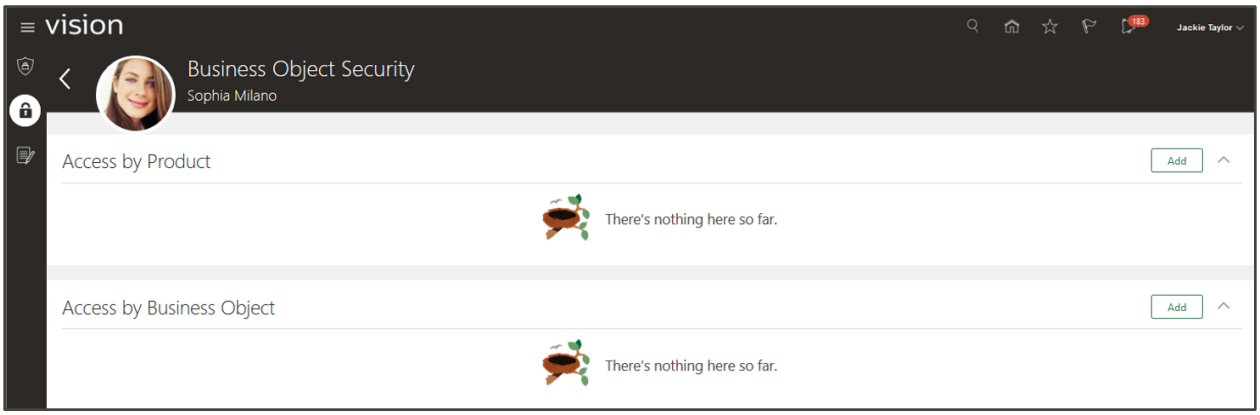


When selecting the user name, a guided process begins, giving you the choice to manually define business object access, or copy another user's data access. This user will be defined to access business objects for payables invoices, related to procure-to-pay processes.

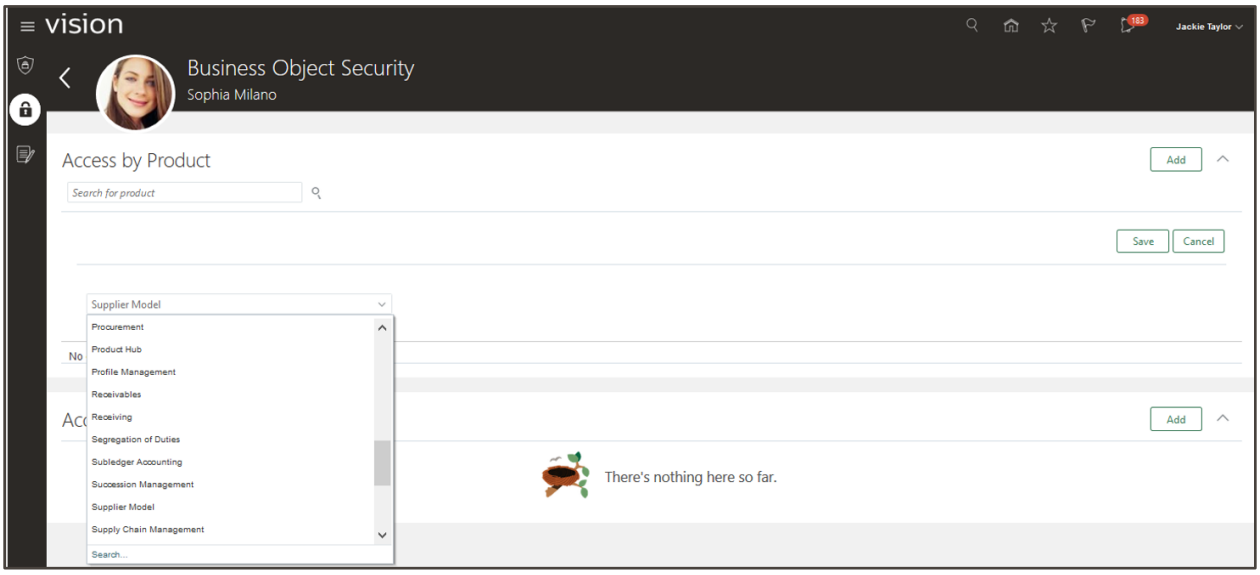
Select the Add option on the Business Object Security page for selected user.



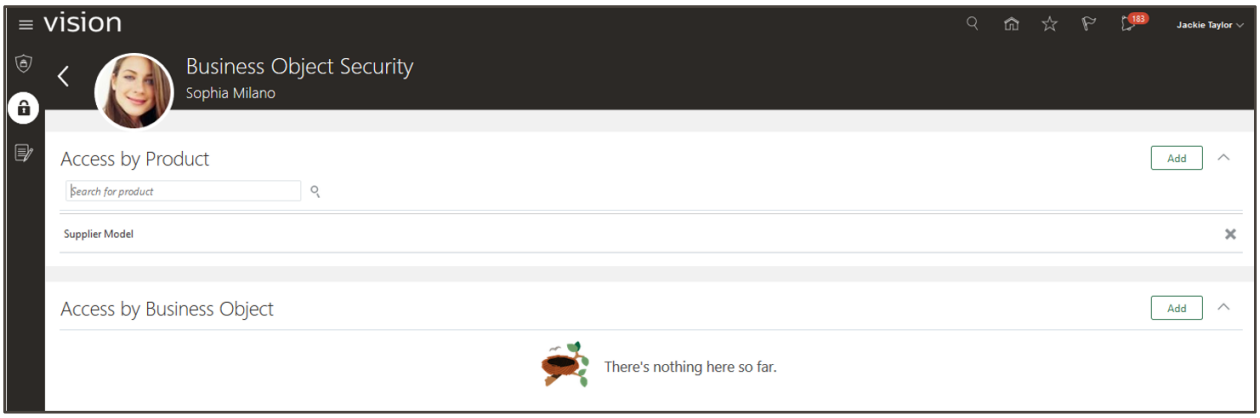
You can define the user's data access by product area or business object. Here in this example, select the Add button for 'Access by Product' region.



All business objects delivered in Advanced Control are related to a Product name, typically representing a functional area such as Payables Invoice, General Ledger, or Supplier. To align with ERP transactions related to suppliers, select the 'Supplier Model' product area, and Save the selection.

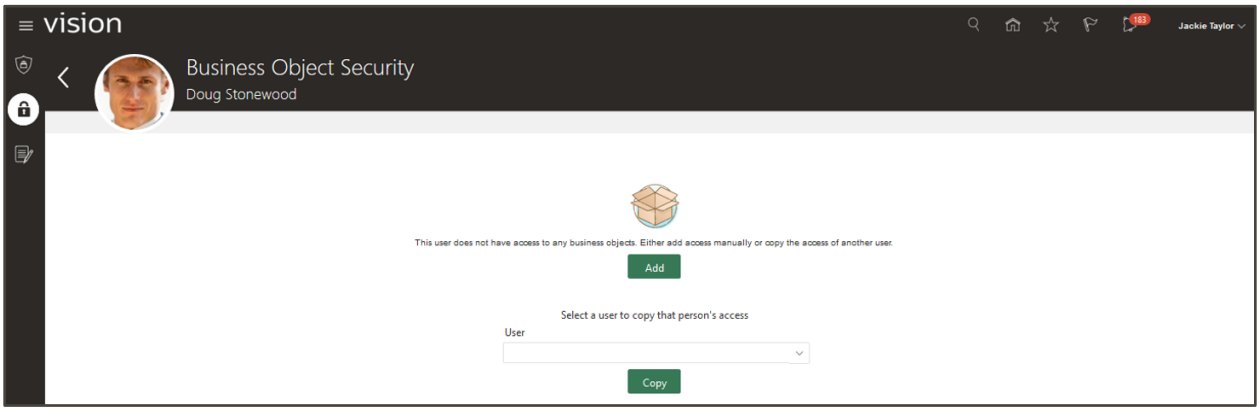


Now you have a user associated to a Product, where they can view, edit, or own models and controls that contain business objects associated to this product area.

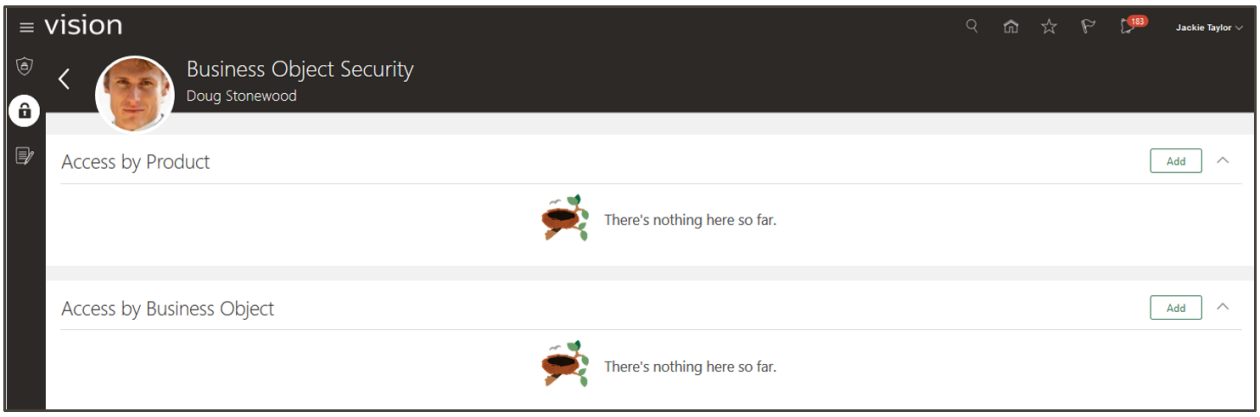


In this next example, let's define a user's access by business object instead of product.

Again, select the Add option on the Business Object Security page for selected user.



Here, select the Add button for 'Access by Business Object' region instead.

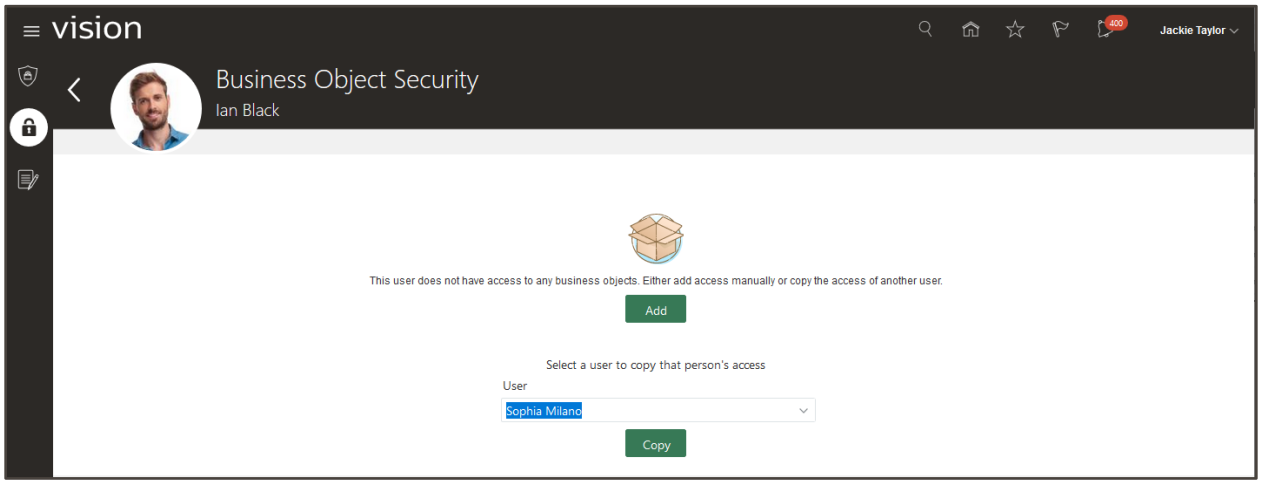


When you know which business object(s) you need to assign, search for them by name. In this example, we want to grant a user business object access to monitor transactions involving payables invoices. Search for 'Payables Invoice', and Save the business object selected.

You can continue to add additional business objects to the user where required.

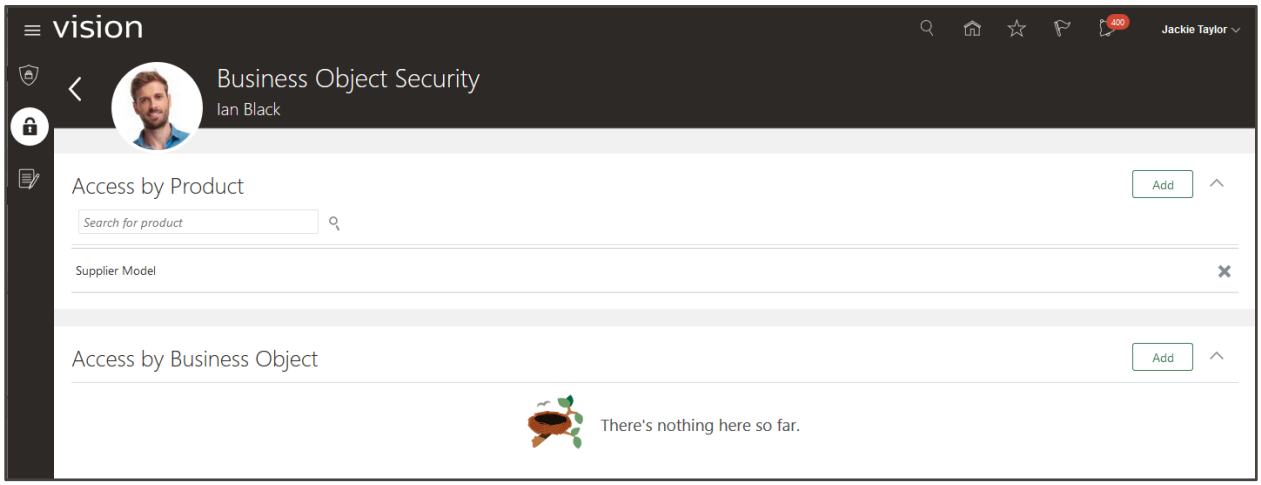
Finally, this example shows you how to leverage a user's existing data security to apply to another user with the same access requirements.

After you select the user's name on the Business Object Security page, in the second half of the page there is a drop-down to select a user name to copy their access. Once you select the user name, select the 'Copy' button.

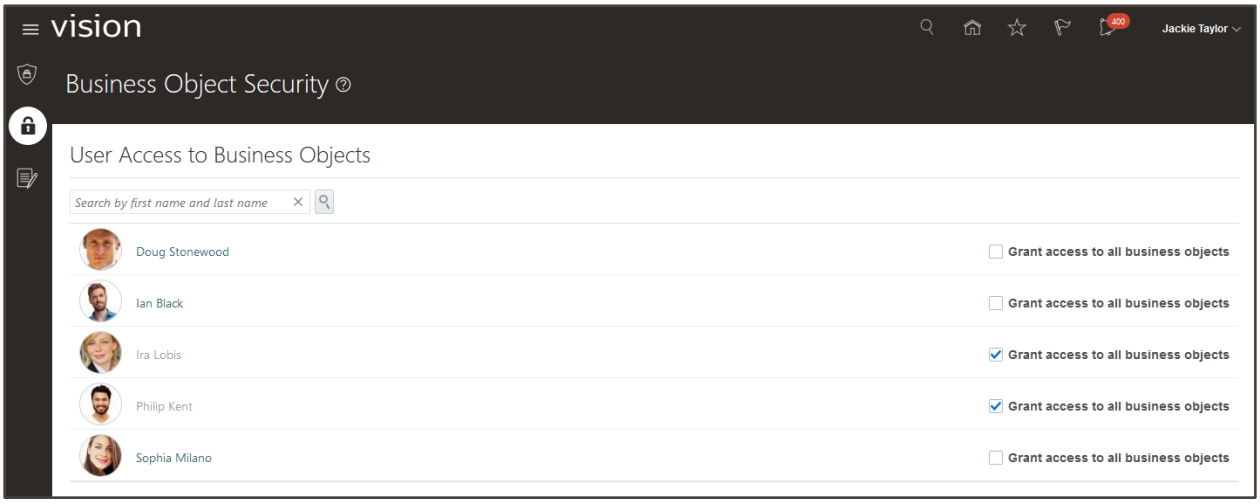


You can leave the data security as-is once copied, or add additional business objects or product areas. Return to the business object security page to review user access.

NOTE: This copy is as of the time the copy is performed and is not a continual synchronization of access between users.



Continue to update any other users with their business object access to complete this step.



As your project evolves, you can always come back to modify a user's business object access. Changes made here are immediate and not dependent on running any security job.

Step 2: Create User Assignment Groups

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

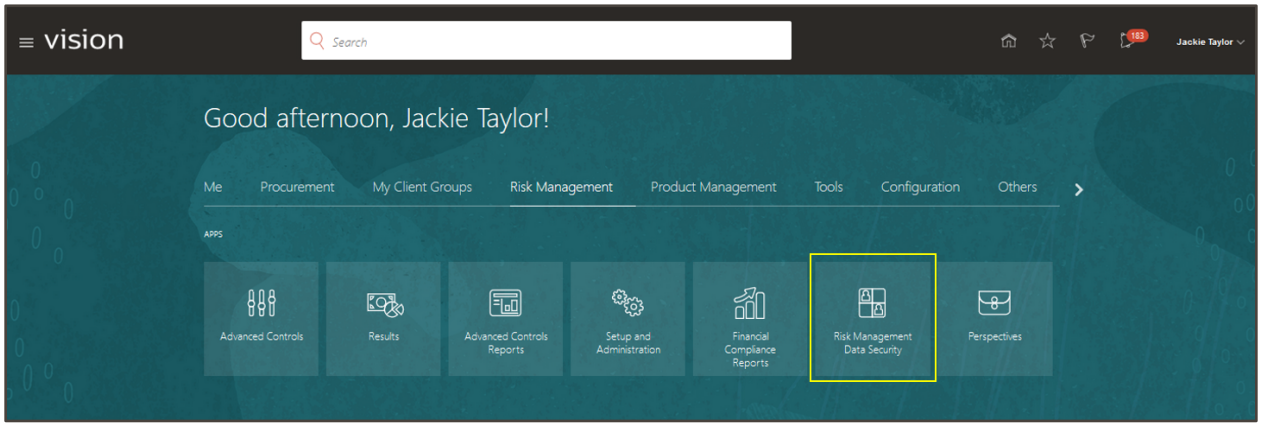
As an overview of this feature, a user group represents one type of data authorization. The criteria includes the data records you can access (objects), and how you can work with the data (authorization). For purposes of this document, there are three object areas we will use here: Transaction Model, Transaction Control, and Transaction Incident. There are also three authorization types:

- Owner – An owner will be able to create and manage an object, including Security Assignments, and access to do so requires the corresponding 'create' privilege associated to the object. Only owners can update Security Assignments by object.
- Editor – An editor will be able to update an object and access to do so requires the corresponding 'edit' privilege associated to the object. Editors can only view Security Assignments by object.
- Viewer – A viewer will be able to view an object and access to do so requires the corresponding 'view' privilege associated to the object. Viewers can only view Security Assignments by object.

Note: When you work with models or controls, you also require business object data security with your owner, editor, and viewer authorization. Business owners accessing incident results generated from a transaction control do not require this business object data security. Additionally, any user or data security you overlooked in the last step, you can go back to update at any time. These steps do not validate against the user's business object data security.

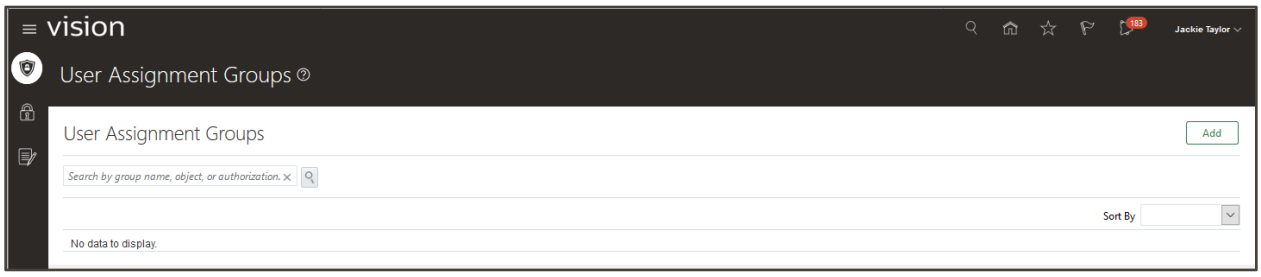
User assignment groups are created and maintained by the risk and compliance administrator. The below will walk through defining user groups for owners in the procure-to-pay business area for transaction controls.

To define a user assignment group, navigate to Risk Management > Risk Management Data Security.

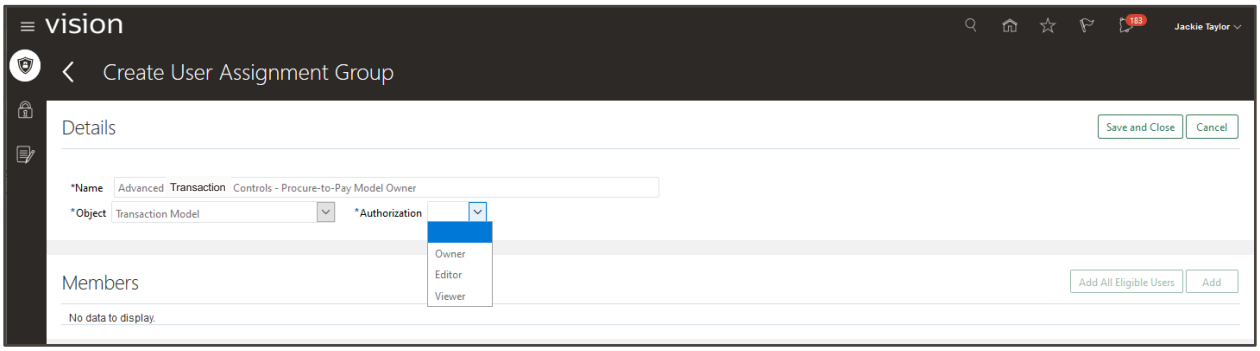


User Assignment Groups for Models

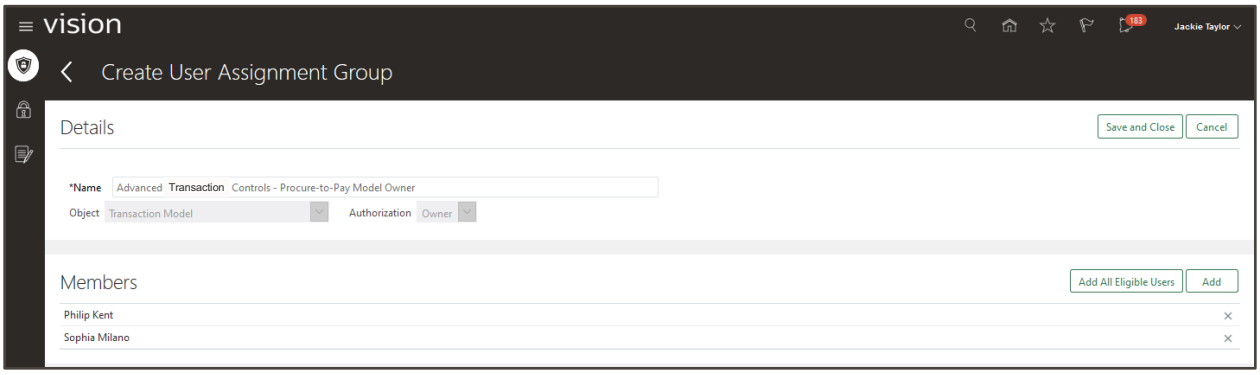
On the User Assignment Groups tab, select the Add button to create a new user assignment group for transaction model owners.



Enter a unique Name for your user assignment group, and select ‘Transaction Model’ object, and authorization of Owner. In this example, the new group is called “Advanced Transaction Controls – Procure-to-Pay Model Owner” and will group members who can create, edit, and assign security for transaction models for that business process.



Next, in the Members section, click Add and select one or more members. (In the Members region of page, you can optionally add all users with this authorization access by selecting ‘Add All Eligible Users’.) Only users with the privilege to ‘create’ transaction models will be available / visible as Members.



When you have finished defining the group for model owners of the procure-to-pay business area, Save and Close the page.

User Assignment Groups for Controls

On the same User Assignment Groups tab, select the Add button to create a new user assignment group for transaction control owners.

Enter a unique Name for your user assignment group, and select ‘Transaction Control’ object, and authorization of Owner. In this example, the new group is called “Advanced Transaction Controls – Procure-to-Pay Control Owner” and will group members who can create, edit, and assign security for transaction controls for that business process.

In the Members section, click Add and select one or more members. Only users with the privilege to 'create' transaction controls will be available / visible as Members.

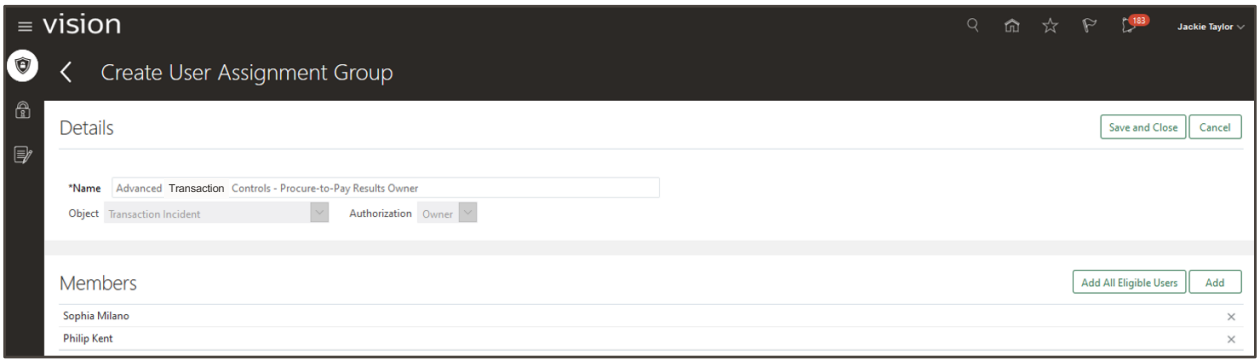
When you have finished defining the group for control owners of the procure-to-pay business area, Save and Close the page.

User Assignment Groups for Results

On the same User Assignment Groups tab, select the Add button to create a new user assignment group for transaction control owners.

Enter a unique Name for your user assignment group, and select 'Transaction Incident' object, and authorization of Owner. In this example, the new group is called "Advanced Transaction Controls – Procure-to-Pay Results Owner" and will group members who can edit and assign security for transaction incident results.

In the Members section, click Add and select one or more members. Only users with the privilege to 'assign' transaction incidents will be available / visible as Members.



When you have finished defining the group for incident owners of the procure-to-pay business area, Save and Close the page.

Note: Members of this group do not require business object data security covered in the previous step, unless they are also a member of either transaction models or transaction controls.

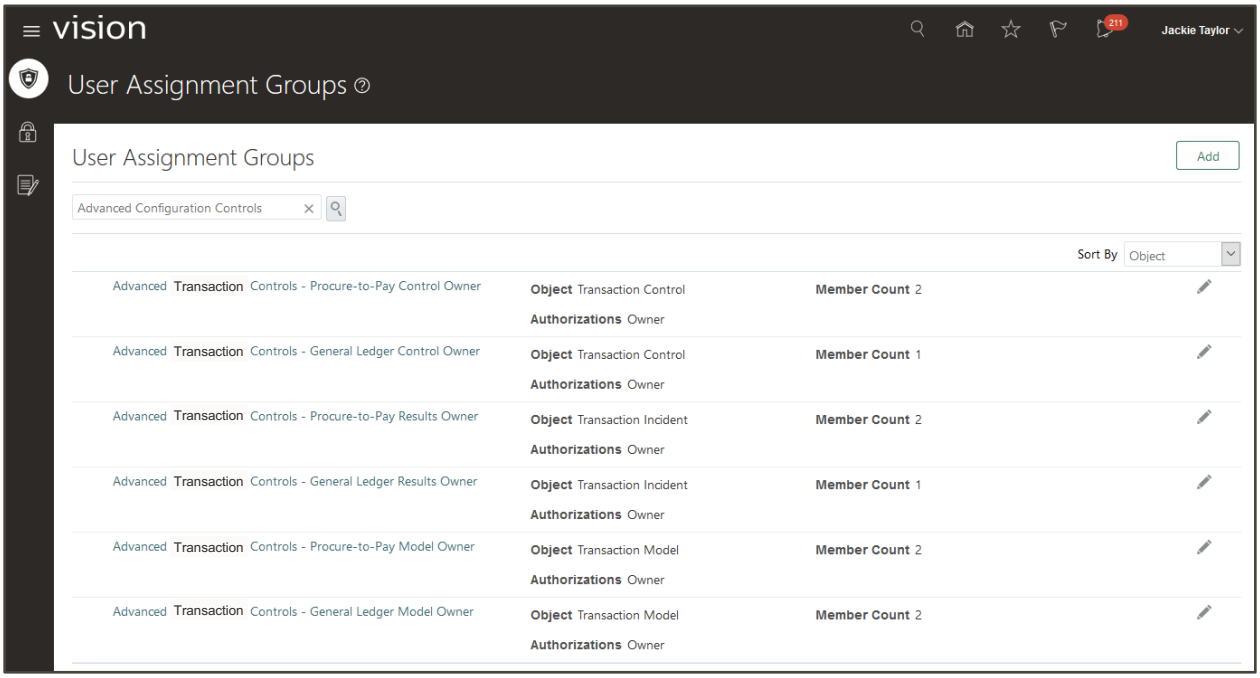
Other User Assignment Groups

In this step, refer to the above examples for defining transaction object 'Owners'; evaluate what additional user assignment groups might be needed in your development environment. You can always come back to update a group's members, or create new groups, as your project evolves.

Other additional groups might include:

- Similar user groups for 'Owner', except different business process users for general ledger instead of procure-to-pay.
- User groups for 'Editor' of models, controls, and incident results.
- User groups for 'Viewer' of models, controls, and incident results.

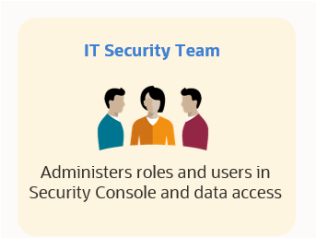
As examples in this document, Owner user assignment groups for general ledger was also defined.



Configure Transaction Models

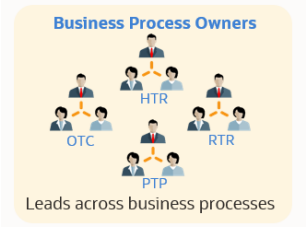
Overview and Participants

This section will cover the steps required to analyze transactions, and leverage this information in Risk Management controls.



Your security team will enable access to configure advanced controls to member(s) of the risk and compliance team.

Your risk and compliance administrator will configure transaction controls in Risk Management. They will also need the 'Advanced Transaction Control Analyst' to import and review the requirements in each model.



Your ERP business process owners will be responsible for providing test transactions and evaluating results.

Step 1: Overview

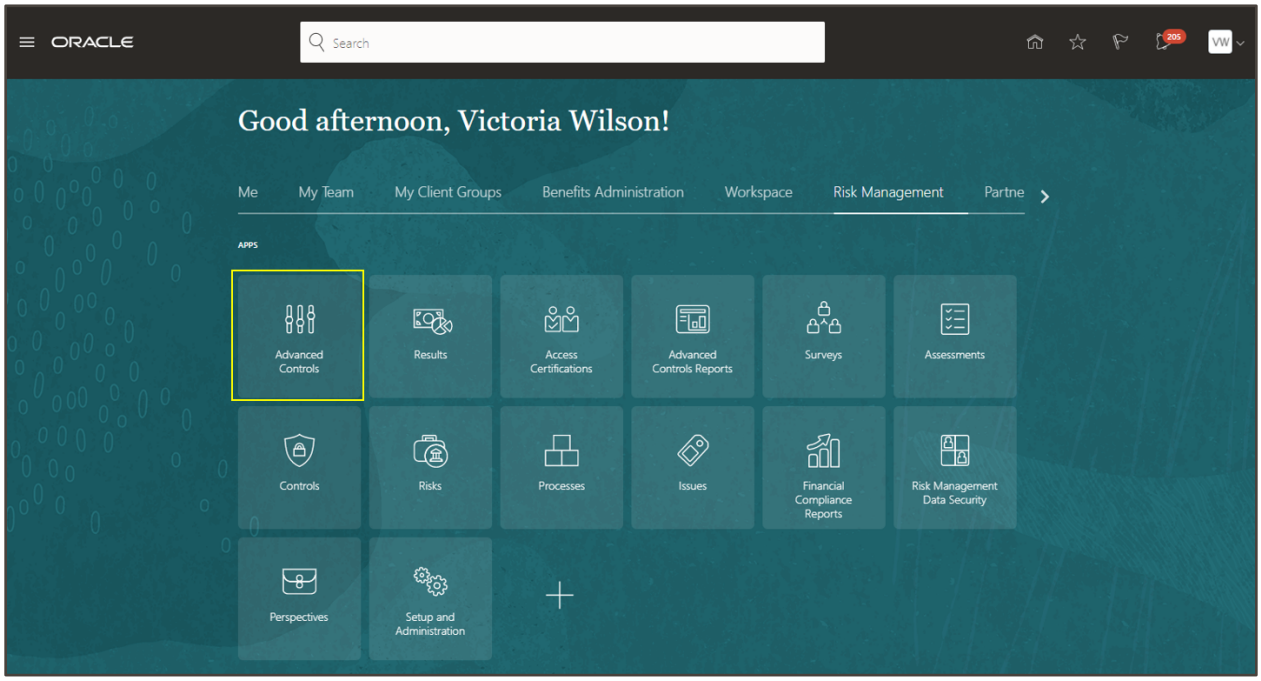
As a prerequisite to using transaction controls in Advanced Controls, you must have access to the business objects that capture the transaction's data.

As reference, let's use the delivered best practice ERP model "30001: Duplicate Payables Invoices" as an example to walk through the configuration process. You will first need to import delivered content from the Advanced Control library to find these transactions.

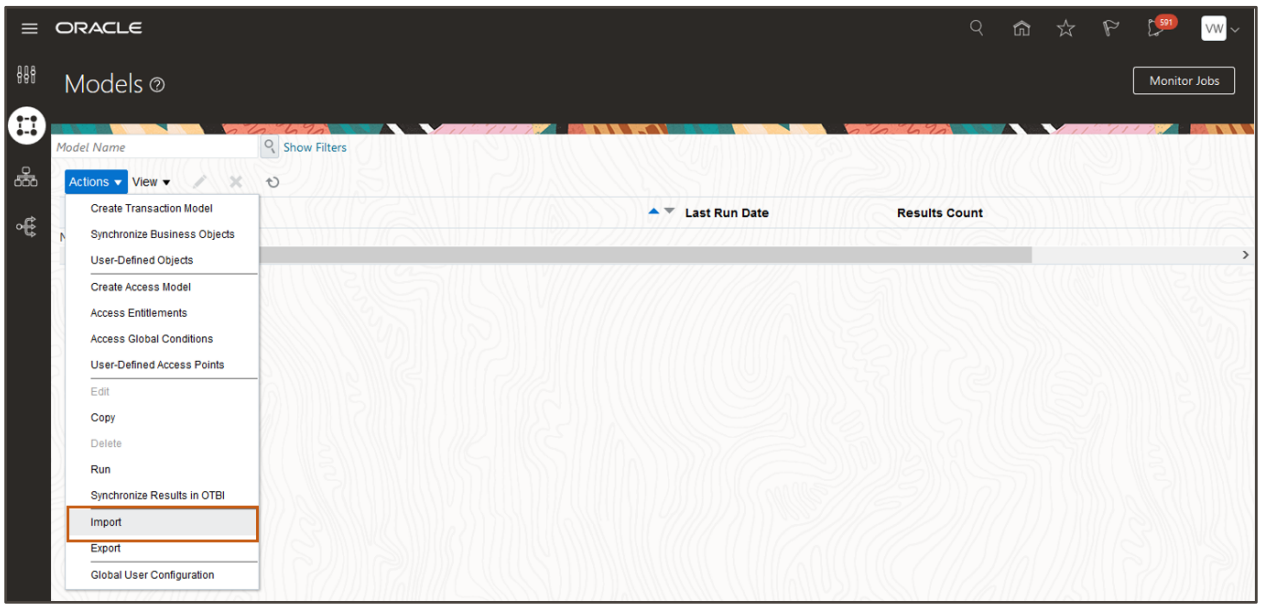
Step 2: Import ERP Models

As a user with owner access to transaction models, you can review the attributes tracked by each model that you import from the ERP content library. The attributes in a business object delivered in Advanced Controls corresponds to an Oracle Cloud business object and attributes visible in Cloud ERP.

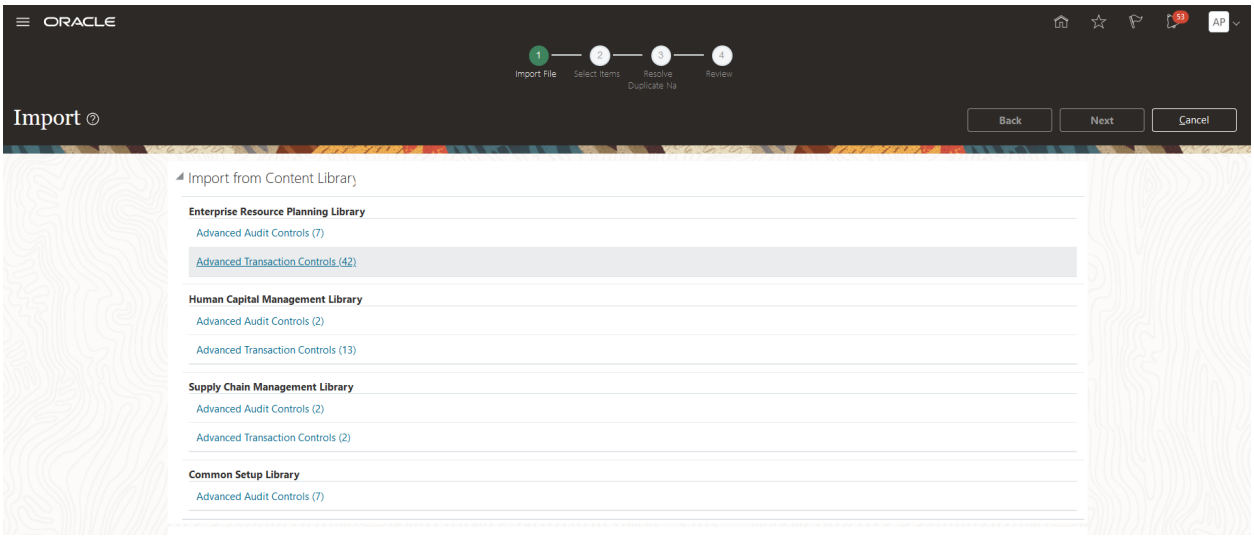
Navigate to Risk Management > Advanced Controls to access the Models page.

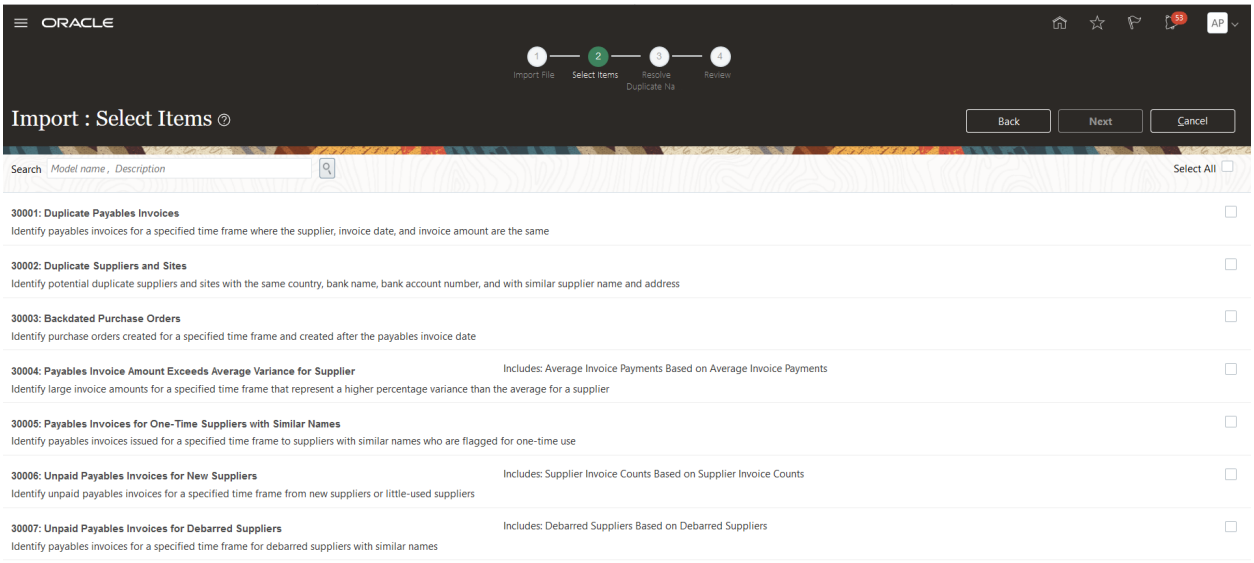


Select the Models tab, and toolbar action to Import from delivered content library.



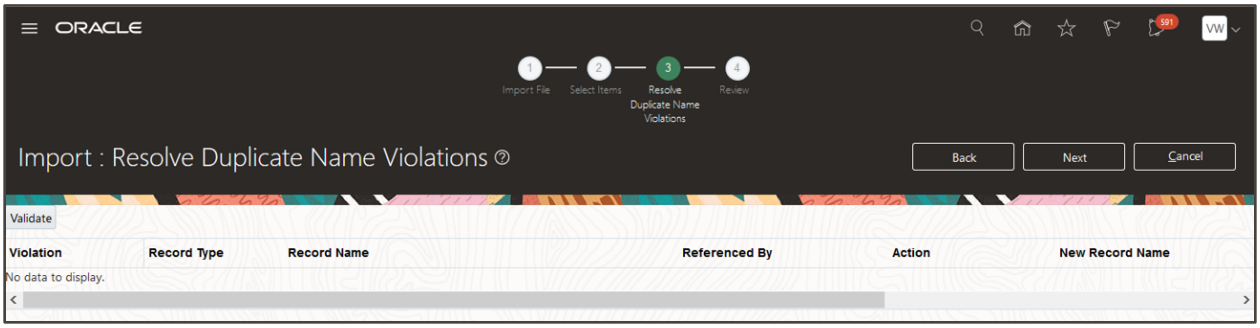
Select the Advanced Transaction Controls link under Enterprise Resource Planning Library (ERP). This will return the available delivered content for this business area.



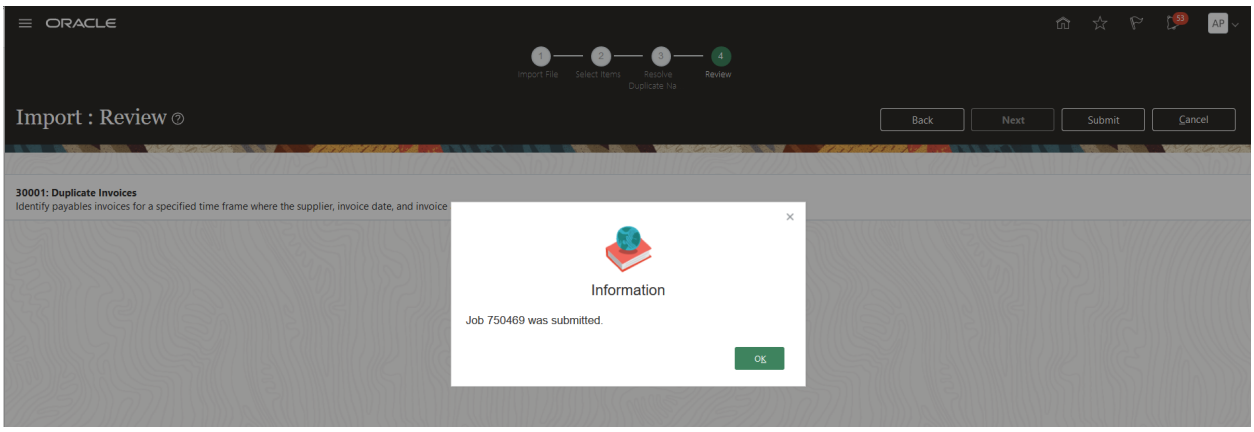


Select “30001: Duplicate Payables Invoices” and click Next.

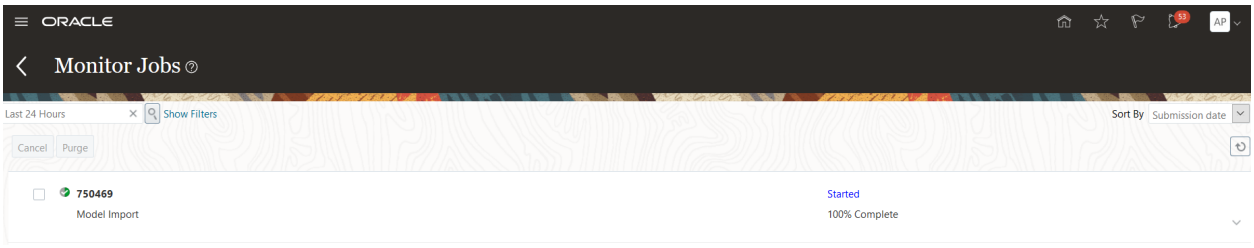
If the delivered model had already been imported before, you will need to Resolve Duplicate Name Violations before moving to next/final page. In this example, this is the first time the models are imported and does not require any action on this page.



Review the selected model and Submit to import it on this final page. A job is run to import the model; note the job ID.



You can check the job status and confirm that the selected model imported successfully by accessing the Monitor Jobs page from Model tab. Click on the ‘Status’ value to review job details (this is the Completed status in below example, where the models was imported).



Note: The user who imports the model automatically becomes its owner.

After you have finished importing the model, proceed to the next step to review it.

Step 3: Review the Transaction Model

For this step, we will continue to use the "30001: Duplicate Payables Invoices" as an example to walk through requirements.

While still on the Model page from previous step, select the 30001 model and click the Edit pencil. In general, a transaction model definition has six key areas:

1. Model name and description
2. Security Assignment in the header region
3. Model Objects
4. Model Logic
5. Model Results
6. Perspective Assignment

Note: Areas like Model Logic and Perspective Assignment details are not covered in this document; you can refer to Other References for related help guides in these areas.

In this step, focus on Model Name (#1): for this and future models, rename the model to include a business process prefix – in this case, consider using "PTP-". Doing so will help to organize the models by business process area type, secure users for these areas, and organization in OTBI reporting covered later in this document.

Step 4: Enter Some Test Transactions

Business process users who would enter test transactions include those who work with procure-to-pay and general ledger.

In your development environment, add a payables invoice. Then add a second invoice with a slightly different invoice number.

Continue to have your business process owners add transactions in the development environment to provide test data to validate controls and results.

Remember that to include these new transactions in an analysis, a synchronization must be performed whether scheduled or manually initiated.

Update and Test Transaction Models

Overview and Participants

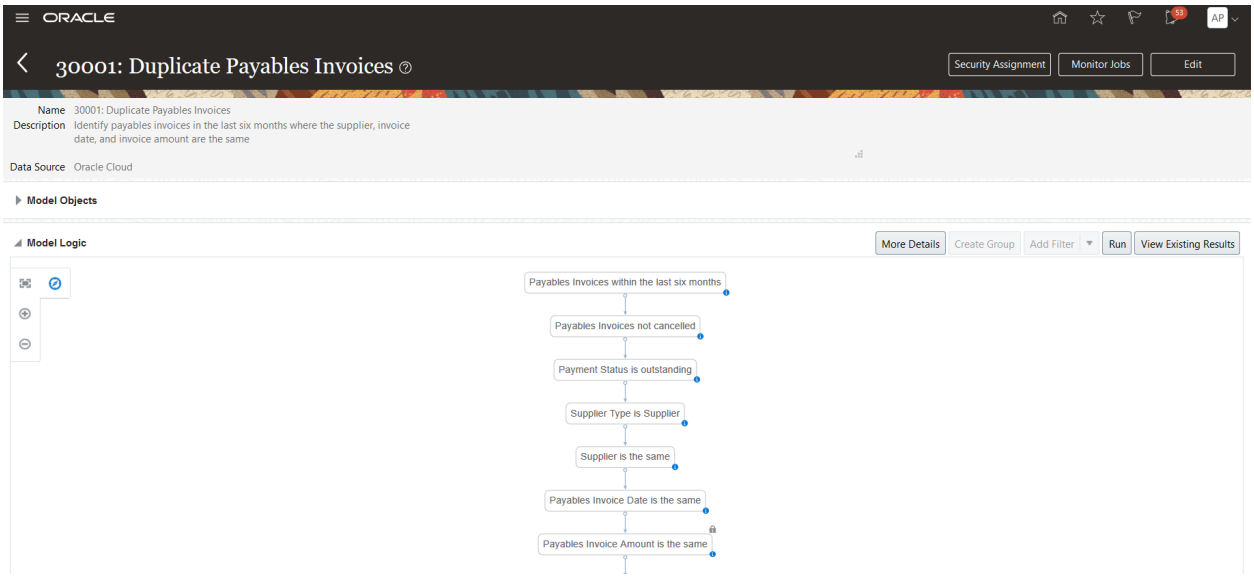
Your risk and compliance team will import and/or create models, deploy and manage transaction controls, and work together with business owners who may also manage controls and incident results. They are responsible for security assignment related to these areas.

Your ERP business process owners will be responsible for validating transaction controls and the incidents they return. They typically are the ones providing requirements for controls, and providing input for security assignment responsibility related to these areas.

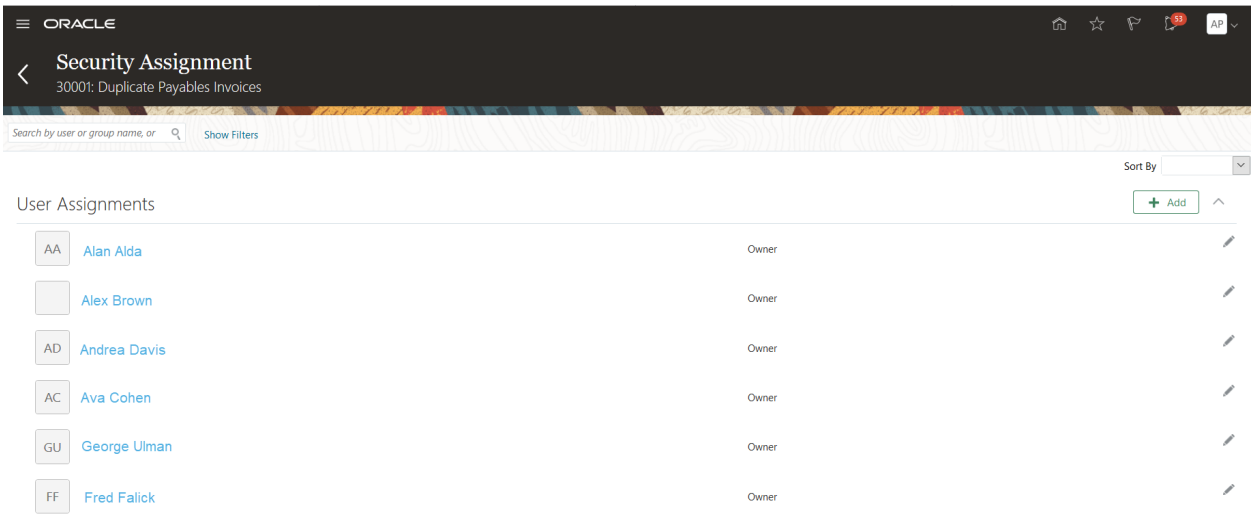
Step 1: Review and Update Security Assignments

As part of this step, go back and review your security group assignments and corresponding business object data security in earlier steps. You want to make sure users working with models and controls going forward have the appropriate authorization and data security.

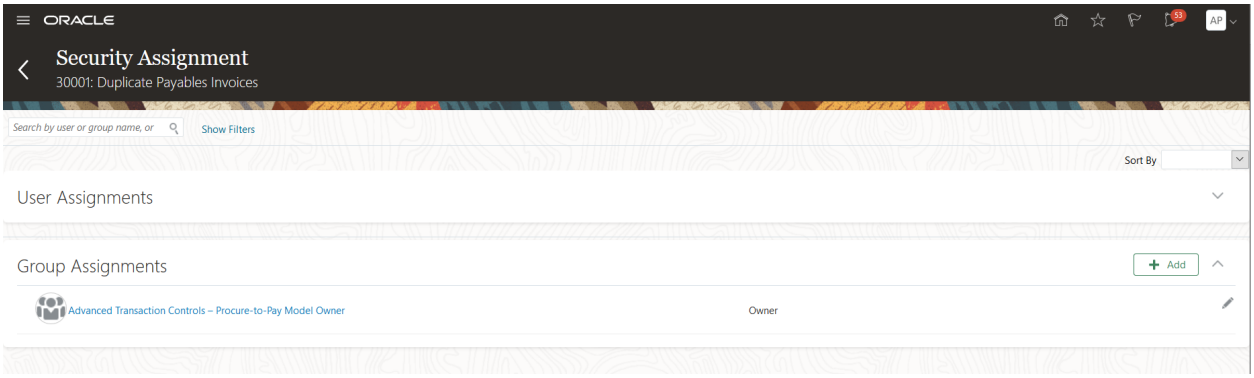
In Risk Management, navigate to Advanced Controls > Models to assign security authorization. Select the model you imported earlier (30001).



Here across from the model name in header, you can update ‘Security Assignment’ to the model definition. Select the Security Assignment button.



On the Security Assignment page for model, under the Group Assignments section you Add the group defined earlier. In this case, it is the “Advanced Transaction Controls – Procure-to-Pay Model Owner” group, and/or a group you have defined for Editor or Viewer authorization based on your requirements and c. (As mentioned earlier, the user who imported the model is defaulted as the Owner; this can be left as-is or changed.)



Consider the following when defining user or group assignments for models in your development environment; they could be different than what you require in production:

- Be sure to involve any other users to evaluate the results, or even those who need to add more test data by granting them access as at least a 'Viewer' of the model results (depending upon their role), and get their feedback on the model's results, because once a model is deployed as a control, you can no longer make changes to the logic or attribute columns returned. (However, you can revise the model again and redeploy as a new control.)
- Alternatively, you can wait to receive the user feedback after the model is deployed as a control and the business process owners can evaluate results in OTBI reports in your development environment.
- It is important that the risk and compliance team work closely with the business process owners who typically sign off on the transaction controls and results tracked.

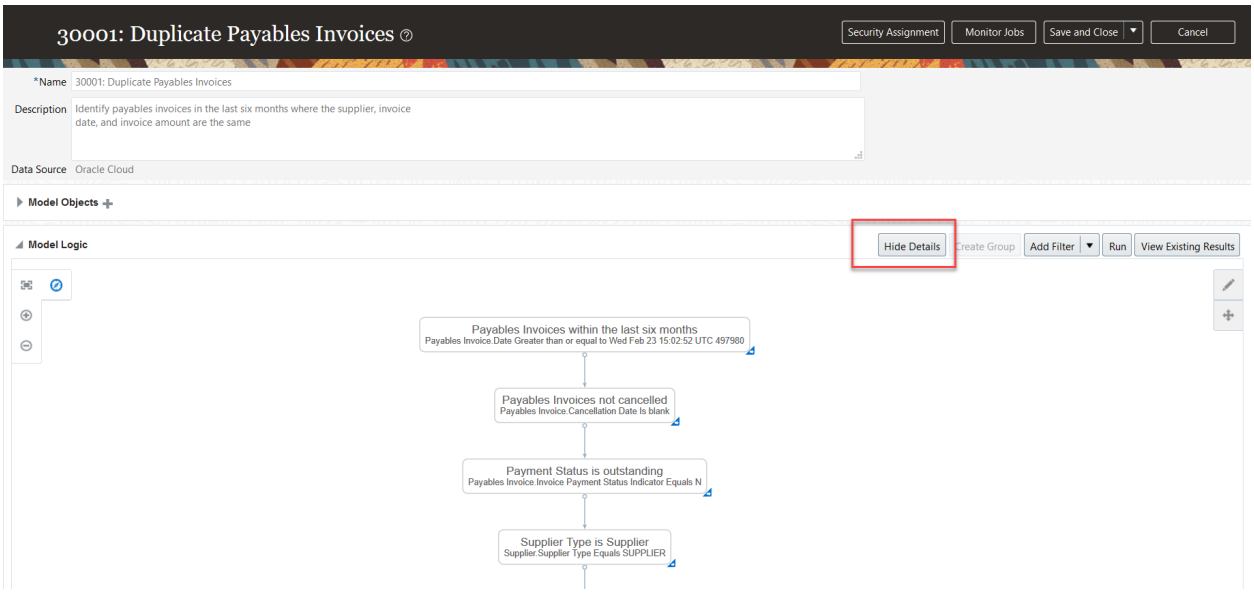
 *Note: Model results are temporary – each time you run the model the results are replaced. Once you deploy the model as a control, each record returned is permanent, with a Result ID that cannot be deleted or replaced, to provide an audit trial of every control incident result returned and tracked.*

Overview of Model Definition

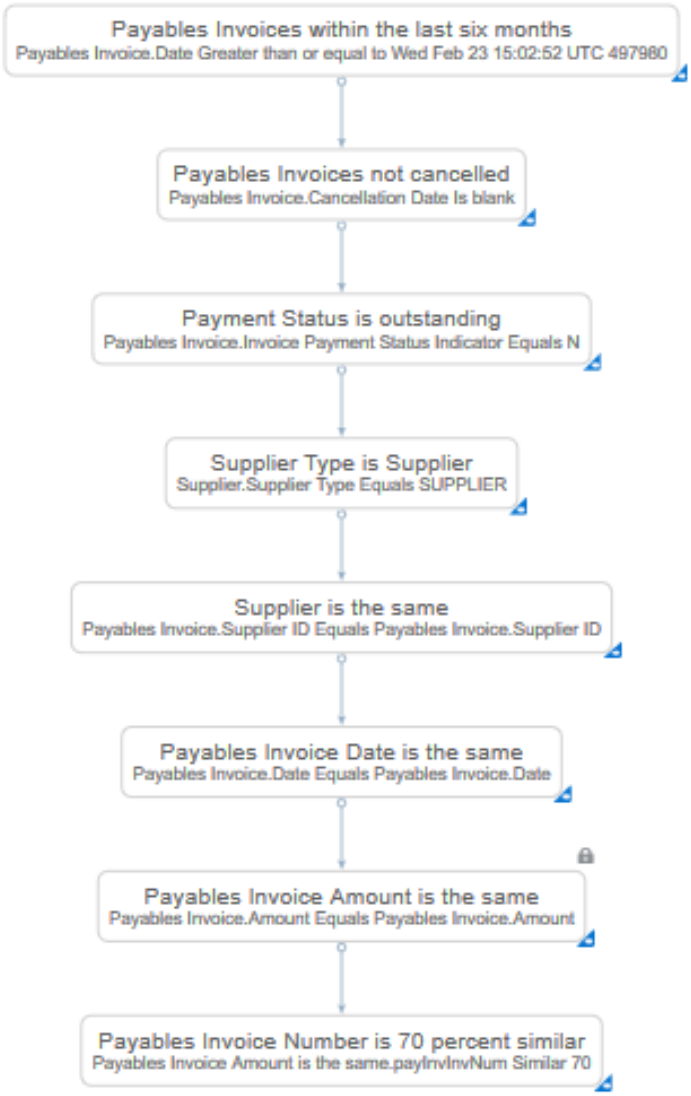
To determine the security and user access to models in a development environment, this section provides an overview of the information you can edit or view in a model.

Each model has a unique Name and includes a Description, Model Objects included, Model Logic, and attribute results to track and report against. Users with Owner or Editor authorization can change any of these areas.

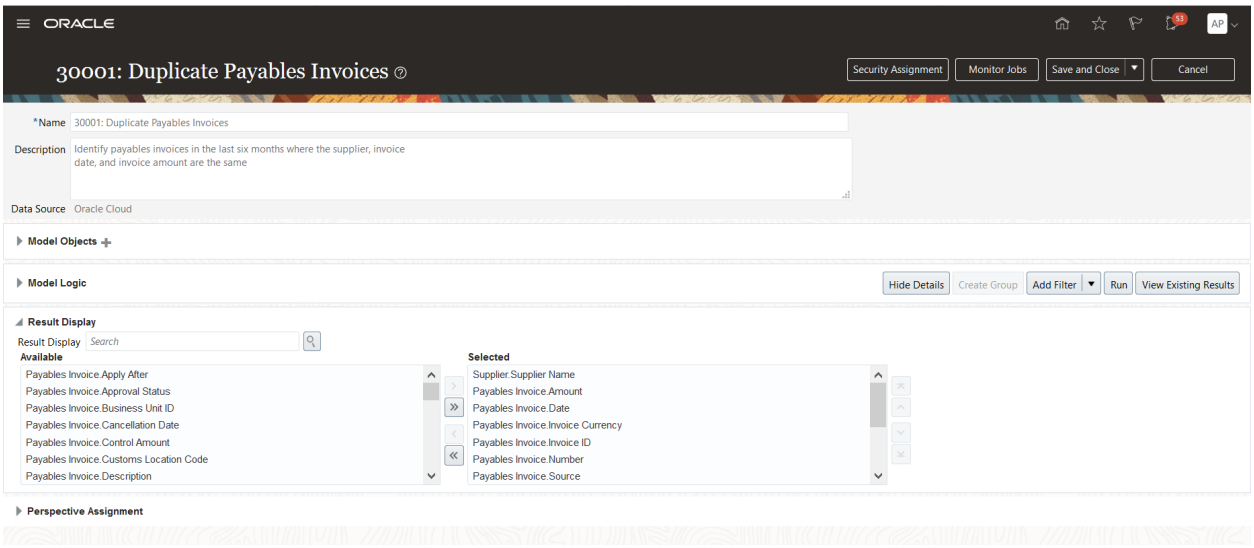
One of the most important sections of a model definition is the logic that provides the rules for incident to be returned and remediated after it is deployed as a control. To review additional Model Logic information, click on 'More Details' button in that region.



If you have owner or editor access, you can open the filter and edit the logic. This document uses the delivered models as-is. For example, this 30001 model includes eight filters:



The Result Display section is where attributes are selected to be returned in results.



For more information on transaction controls and best practices around model design, refer to Related Resources section of document.

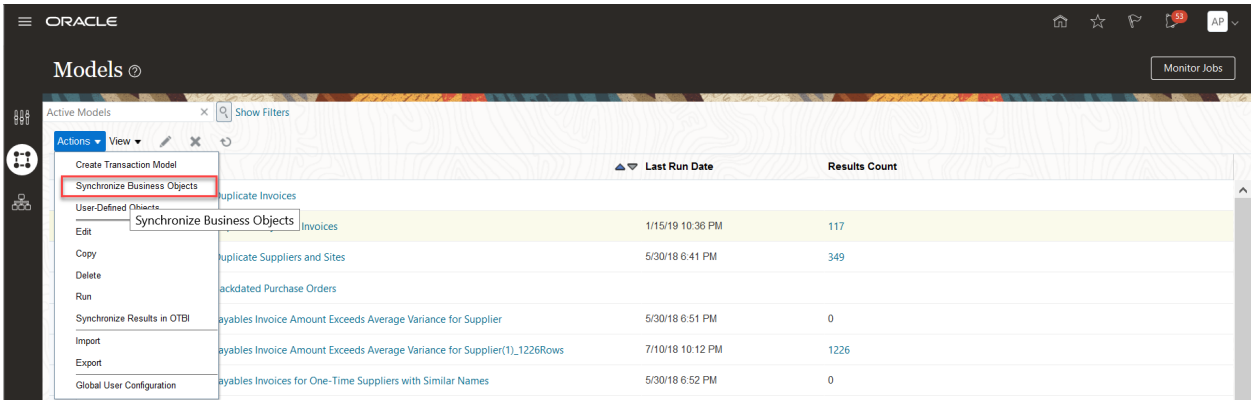
Note: For purposes of this document and any following steps around reporting, we use the delivered model logic and attribute definitions in model.

Step 2a: Run Synchronization for a Model

Your next step is to synchronize the transaction data captured to-date by either running model synchronization, or synchronization for all business objects used.

Using model 30001 as an example to synchronize at the model level, select Actions > Synchronize Business Objects.

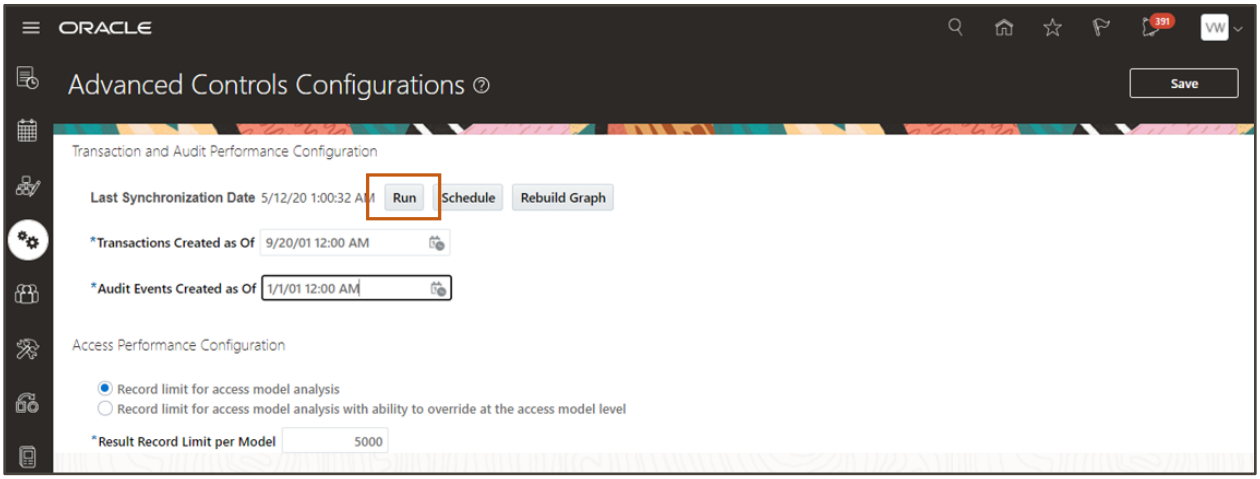
You can only use this option if the business object used in model has never been synchronized before; it does not apply to incremental updates. If previously synchronized, perform Step 2b instead.



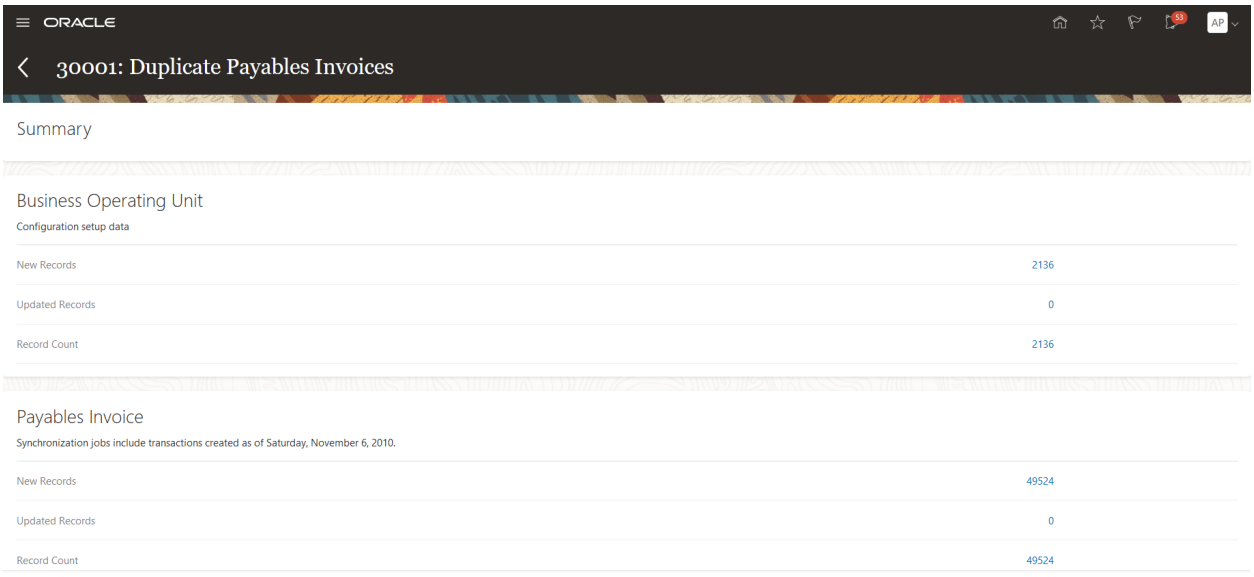
Step 2b: Run Synchronization for All Business Objects

As a risk administrator, run the synchronization for all business objects used across models and controls. Any business objects used are synchronized; this includes any data updates for business objects already used or those used for the first time.

This job can be put on a schedule, as referenced under the Other Activities section. Note the job ID when running synchronization so you can check job status.



Once the job has completed on the Monitor Jobs page, you can drill into the status link to review the record counts by business object that have been synchronized. The summary provides information on new and updated records by business objects.



Step 3: Run Model Results

Run your model and review the data results. If there are no results, create additional test transactions in your development environment, then run transaction synchronization again to update event records for a business objects used.

Step 4: Add More Models

Repeat the previous steps for these models:

- Procurement
  - 30003: Backdated Purchase Orders
  - 40001: Supplier and Payables Invoices Created by the Same User
  - 40004: Payment Process Request Created by Same User Managing Suppliers
  - 40005: Suppliers and Purchase Orders Managed by the Same User
- Financial Management
  - 32002: Manual Journals Posted After Period Close Date
  - 40006: Customers and Receivables Invoices Managed by the Same User
- Self-Service Financials
  - 31004: Duplicate Expenses Submitted by Employee for Reimbursement
- Supply Chain & Manufacturing
  - 40003: Item and Inventory Transaction Created by the Same User

Deploy and Run Transaction Controls

Overview and Participants

Your risk and compliance team will deploy and manage transaction controls and work together with business owners who may also view or manage controls, and monitor incident results.

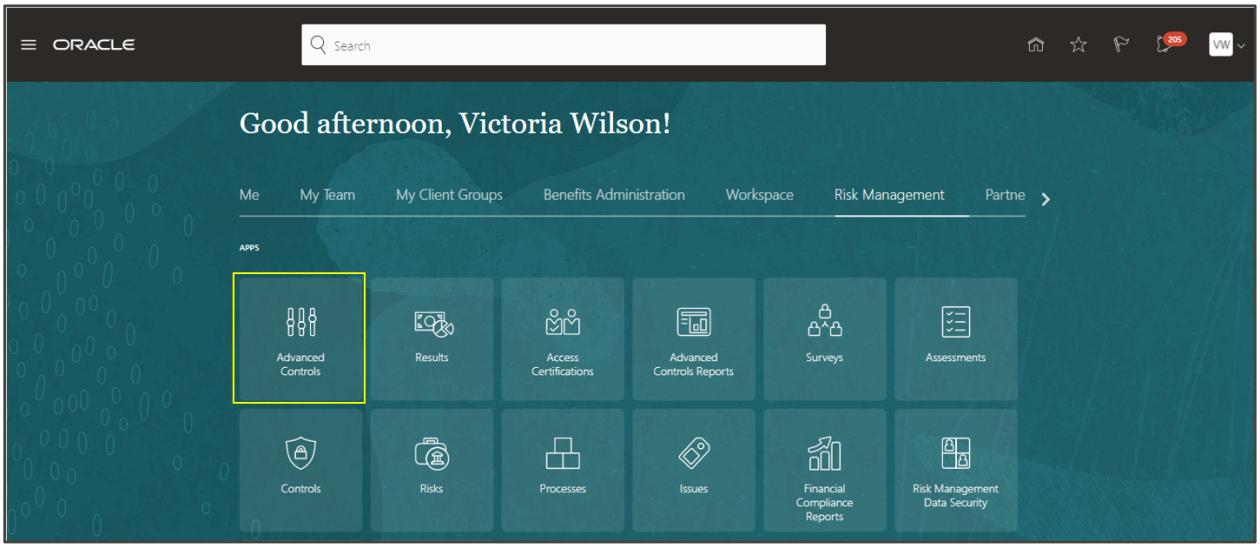
Your ERP business process owners will be responsible for validating transaction controls and the incidents they return. They typically are the ones signing off on controls to promote to production, and finalizing security assignment responsibility related to these areas.

Step 1: Deploy Transaction Controls

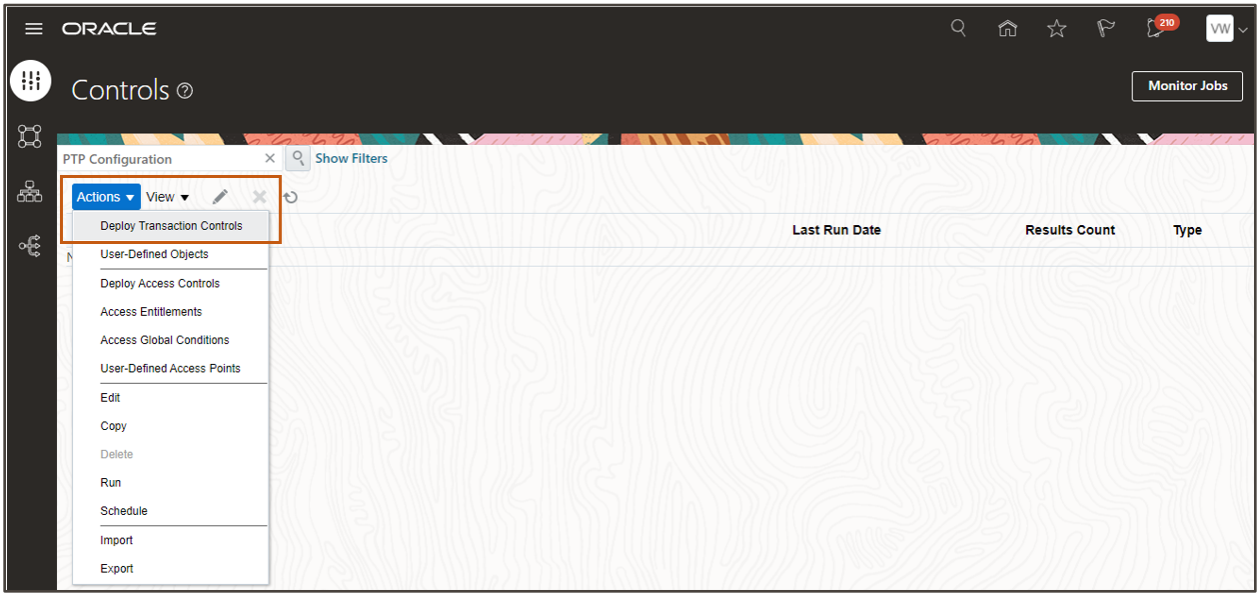
Based on collaboration between your risk and compliance team, and the business process owners input, deploy models as controls to test continuously monitored transaction events in development and eventually production.

Before proceeding, it is important you evaluate your user assignment groups for Transaction Control and Transaction Incident object types to avoid significant mass updates to include users involved in evaluating these transaction controls for production. Also, confirm any Transaction Control users have the required business object data security discussed under Risk Management Data Security. (The users evaluating only control incidents do not require data security at the business object level.)

To deploy transaction controls, navigate to Risk Management > Advanced Controls.



On the Controls tab, select Actions > Deploy Transaction Controls to select the models to create transaction controls.

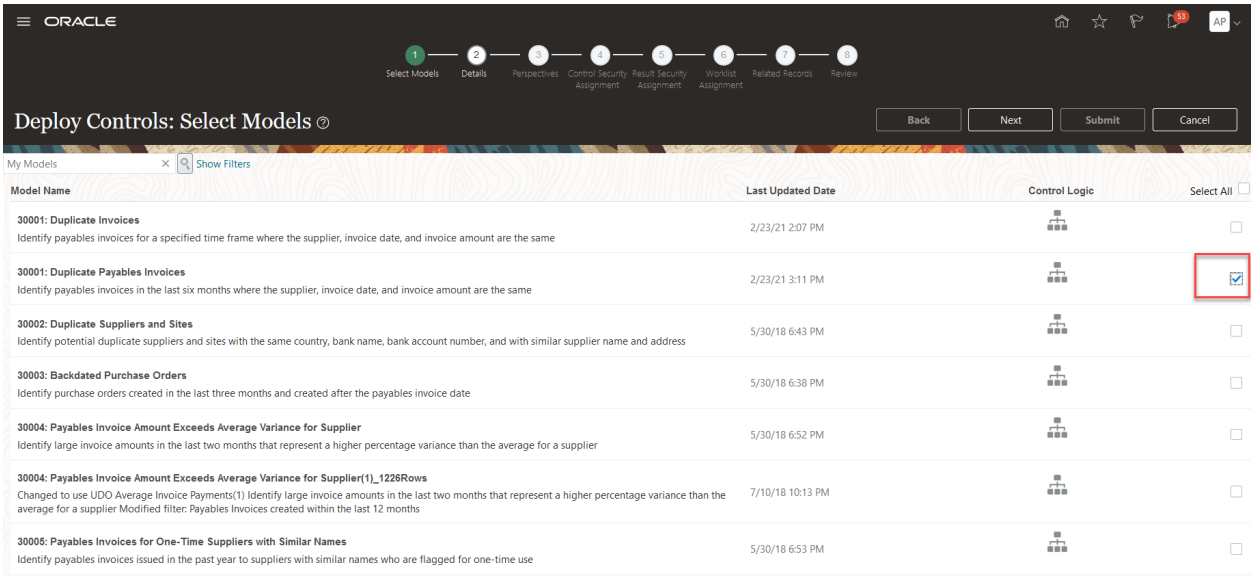


The following sections cover each of the train stops – or page - to select and deploy transaction controls.

Select Models

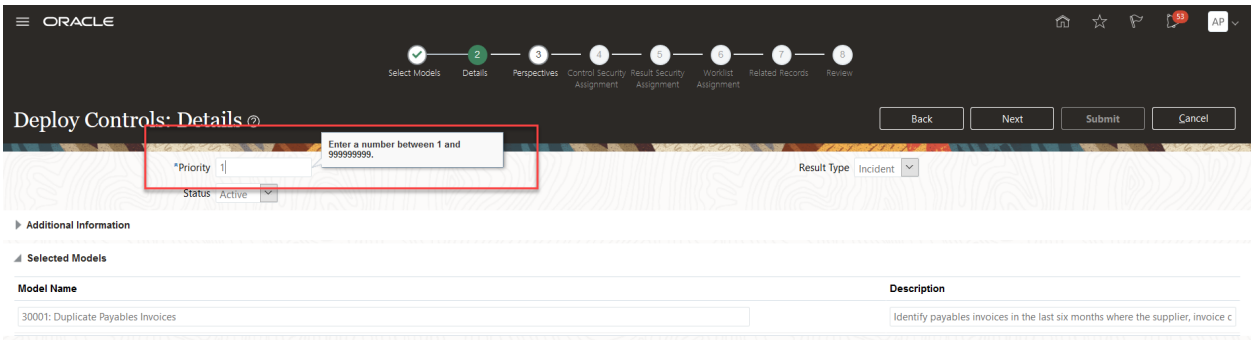
Select from an available list of transactions models to create controls. In line with previous steps, search and select the five models covered in document. You can select one at a time to create a control when criteria differs, such as priority or user assignment groups for general ledger versus procure-to-pay.

The following examples uses one model as an example to deploy as a control: 30001. Select Next to proceed.



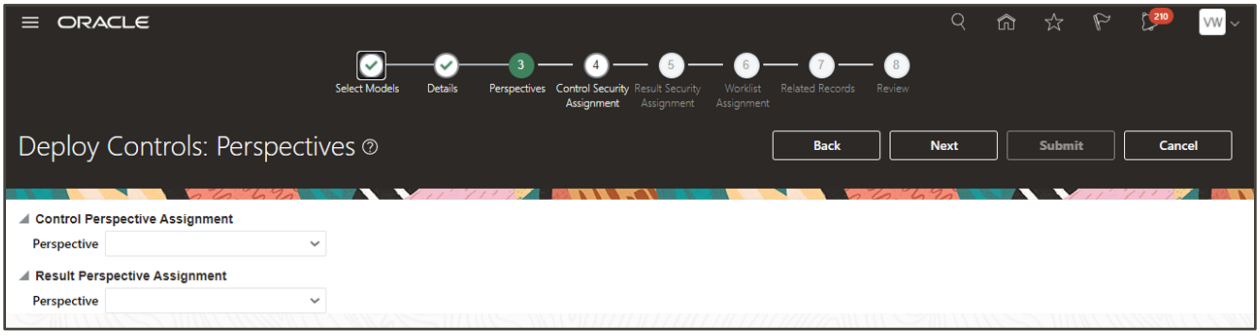
Details

On the Details page you can set the Priority of the control; do not change the Name or Description of the control. You are defining an 'Incident' Result Type. Select Next to proceed.



Perspectives

When you use Perspectives, the information is used in conjunction with reporting. Often one perspective around business processes is defined in Risk Management. However, this feature will not be covered in detail and you can refer to Related Resources section. Select Next to proceed.

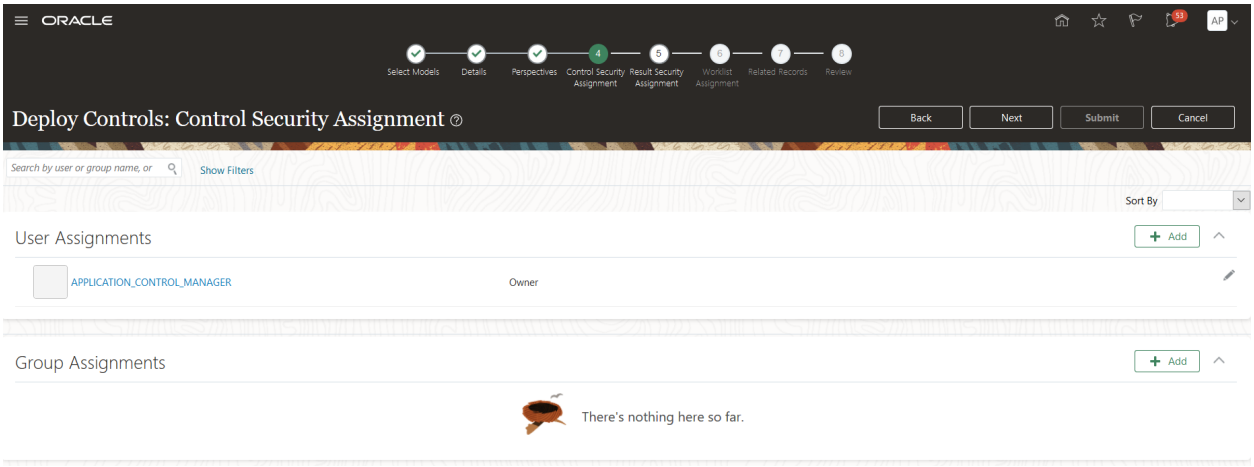


Control Security Assigment

The user deploying the control defaults as an Owner. Use this Control Security Assignment page to apply your user assignment groups covered earlier in this document. The selection may include one to many, depending upon your business process and required authorization types (owner, editor, or viewer).

Users or groups assigned on this page require the corresponding business object data security used by the control. This can be updated after creating the control if data security is missing.

After selecting Save, select Next to proceed.

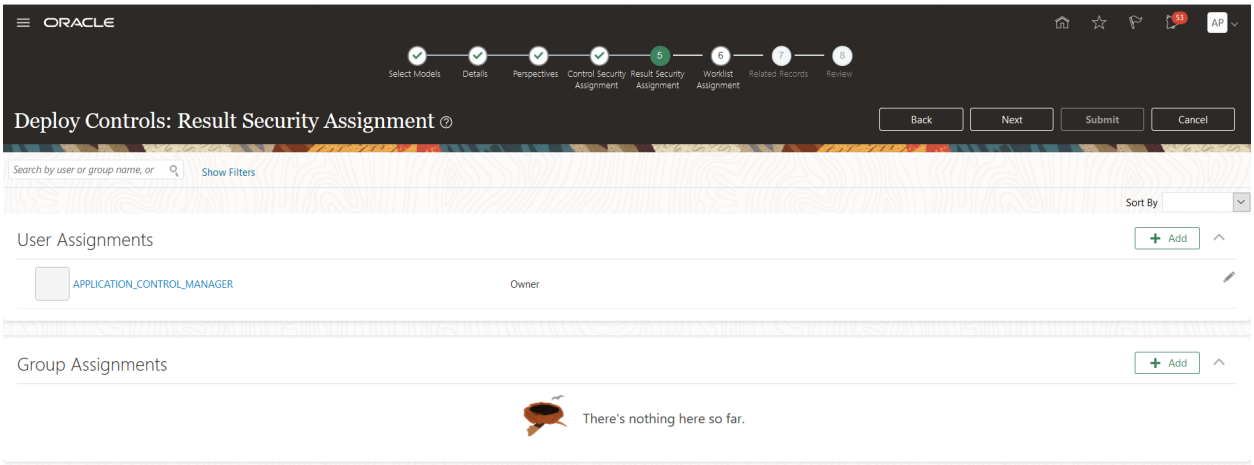


Result Security Assignment

The user deploying the control also defaults as an Owner for result incidents. Use this Result Security Assignment page to apply your user assignment groups covered earlier in this document. Again, the selection may include one to many, depending upon your business process and required authorization types (owner, editor, or viewer).

Users or groups assigned on this page do not require business object data security, unless they are also given authorization to the control.

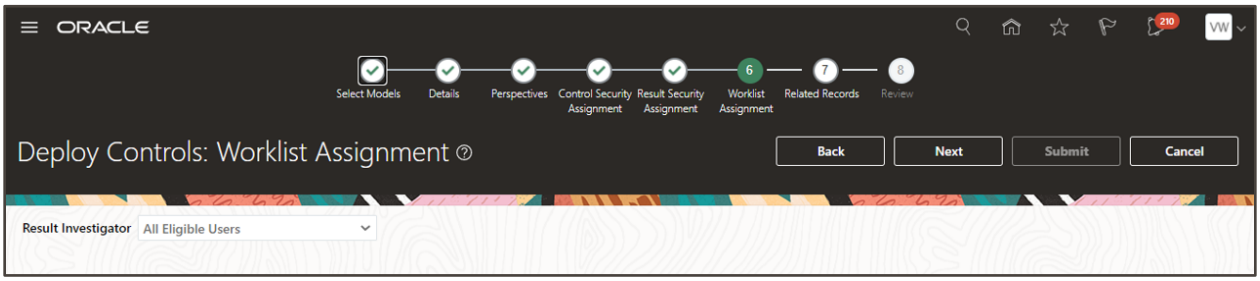
After selecting Save, select Next to proceed.



Worklist Assignment

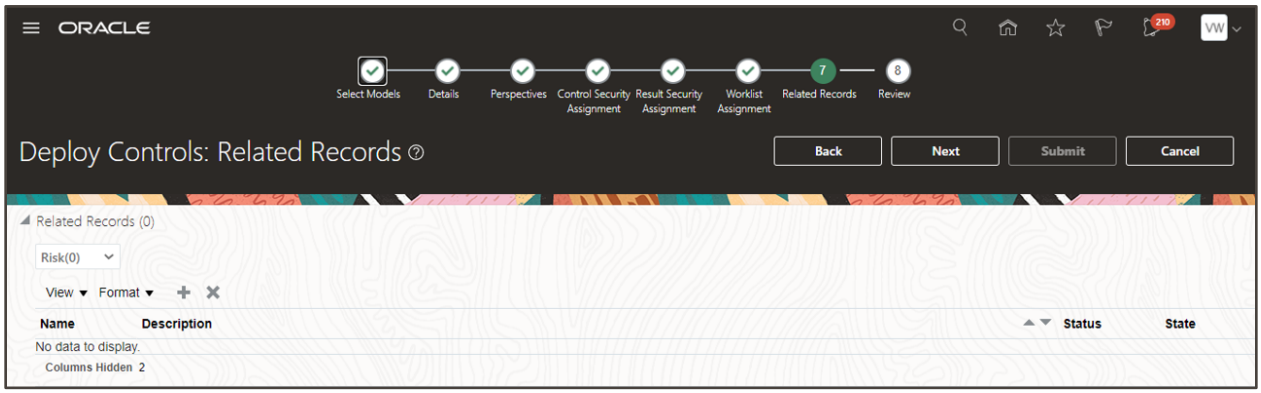
On the Worklist Assignment page you can leave the default to include All Eligible Users to receive a worklist, or assign one user as the primary result investigator. In this case, even though one user may receive the worklist, any user authorized to own or edit can access and update the incidents.

Select Next to proceed.



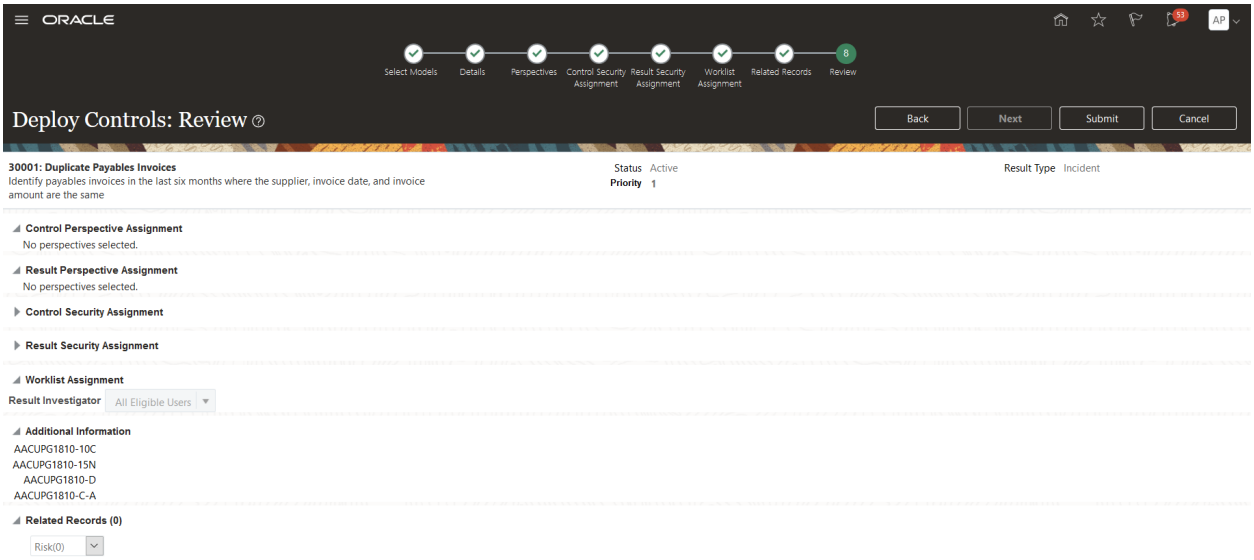
Related Records

When you use Financial Reporting Compliance, you can use the optional Related Records page to link your advanced control to a process, risk, or control. This feature is not covered here in detail, but you can refer to Related Resources section. Select Next to proceed.

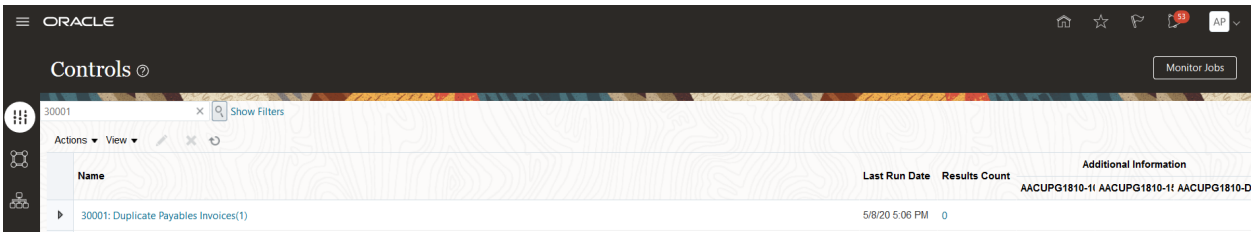


Review

The last Review page to deploy a control provides an overview of all the criteria set; if satisfied, select the Submit button.



Your selected model has now been deployed as a control.



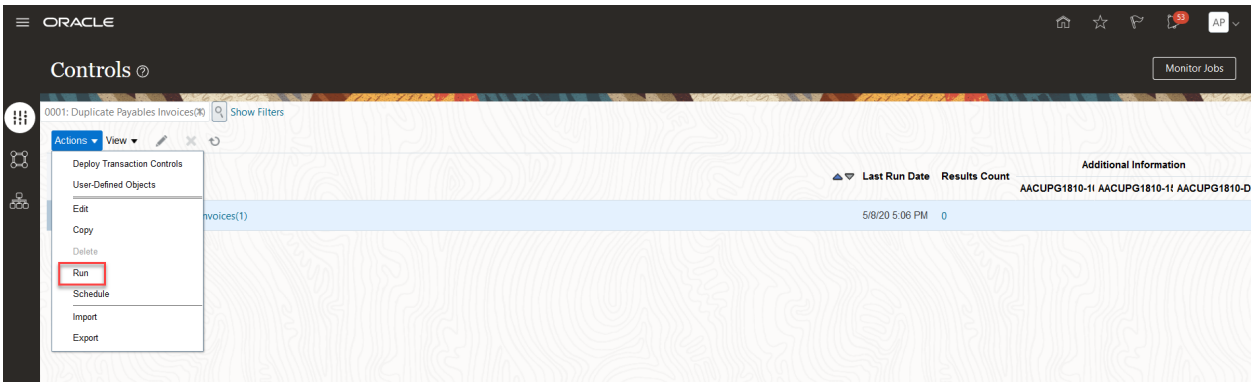
Using these steps, go back and deploy the remaining models as controls. Note you should deploy controls based on those that require the same criteria, such as priority and user assignment groups, because what you define on each page applies to all those selected.

Step 2: Run Data Synchronization

Before running control analysis on your transaction controls, run the transaction synchronization job so the most current data in your development environment is sourced for the next step. Refer to the previous section – Step 3: Run Synchronization for All Business Objects – for information on this job.

Step 3: Run Controls

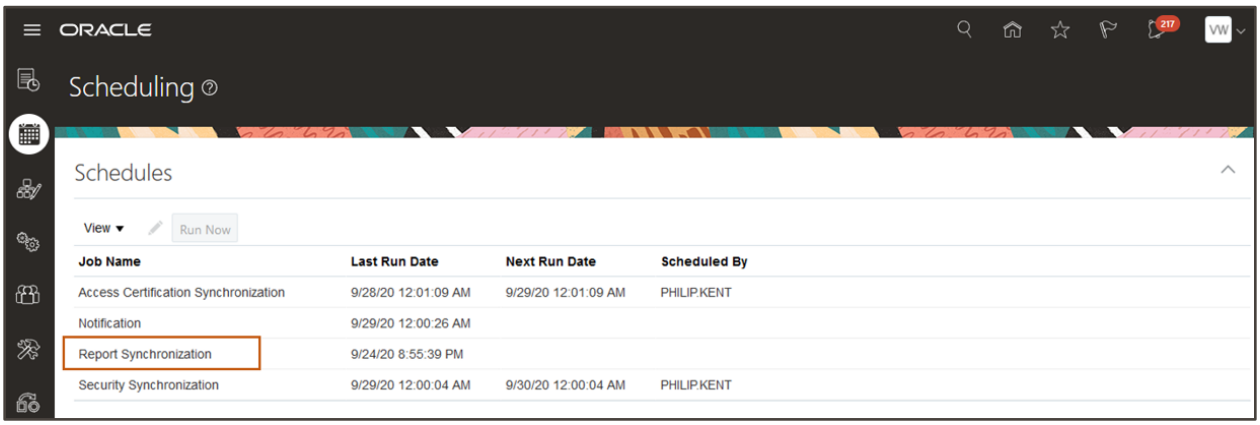
Once the synchronization job is complete, navigate to Risk Management > Advanced Controls to run control analysis. Select one to many controls, then select Actions > Run from the toolbar.



Step 4: Run Report Synchronization

After all your transaction controls have completed, run the Report Synchronization job. This job makes the data available in OTBI subject areas used by dashboards and reports. The transaction controls use the subject area called 'Risk Management Cloud - Advanced Financial Controls Real Time'.

To run this job, navigate to Risk Management > Setup and Administration. Select the Scheduling tab, and then run Report Synchronization.



Once you have completed all the steps in this section, you are ready to deploy the Risk Management Dashboard.

Deploy the Risk Management Dashboard

Overview and Participants

Your risk and compliance team will deploy the Risk Management dashboard and configure the reports in the development environment. Doing so may require assistance from an implementer who has BI administrator access.

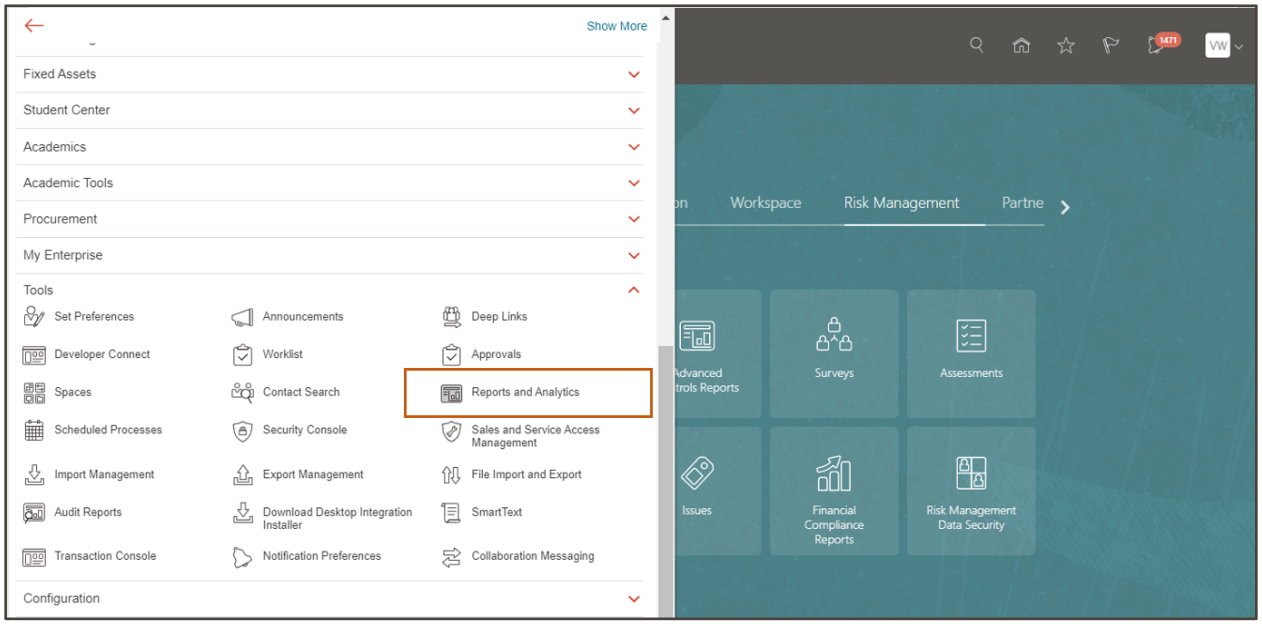
Your ERP business process owners will use these reports and dashboards to evaluate and remediate incident results for transaction controls.

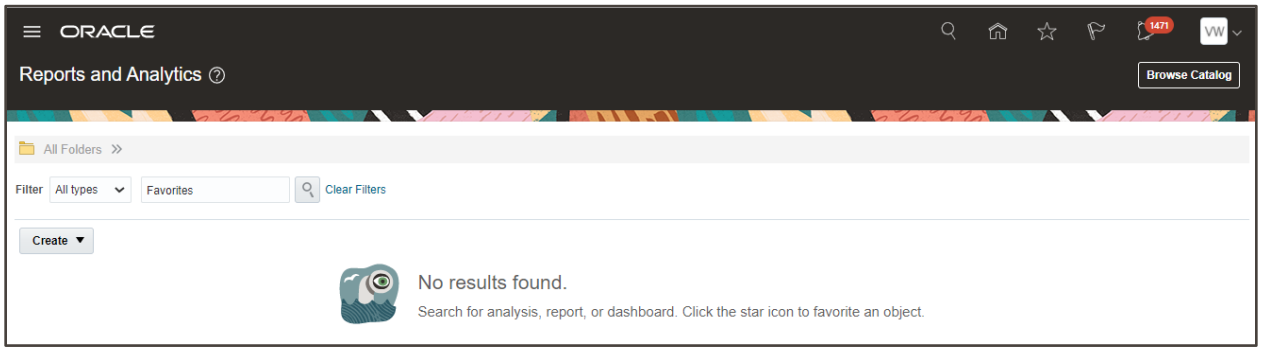
Step 1: Unarchive Risk Management Dashboard

First, go to Oracle's Cloud Customer Connect website to download the Risk Management Dashboard catalog file, found on the Solution Blueprint Dashboards and Reports page. If you have previously unarchived this catalog, follow the recommendation on that website to update artifacts related to Transaction Controls under the '00 Dashboard' and 60 Monitor Transactions', then skip to Step 2.

To unarchive the Risk Management Dashboard for the first time, you must have a job role that grants access to the BI Administrator role. The predefined Application Implementation Consultant job role has this access.

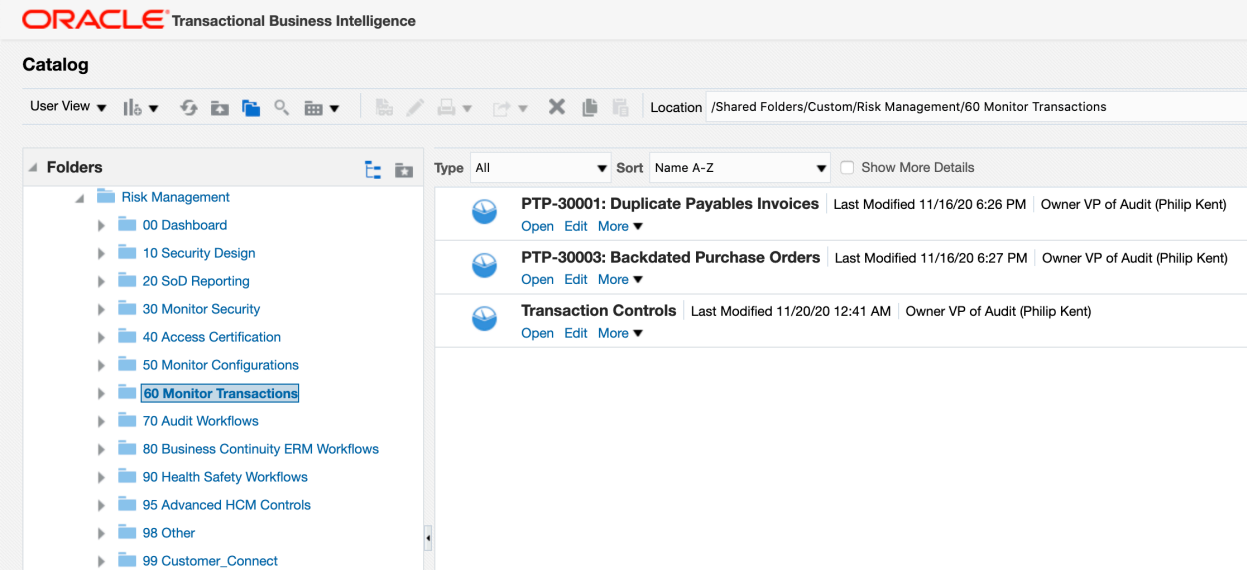
Navigate to Reports and Analytics, and then select Browse Catalog.





Go to Folders, and under Shared Folders select Custom. Then under Tasks, select Unarchive to deploy our Risk Management Dashboard catalog. You will see the new Risk Management folder.

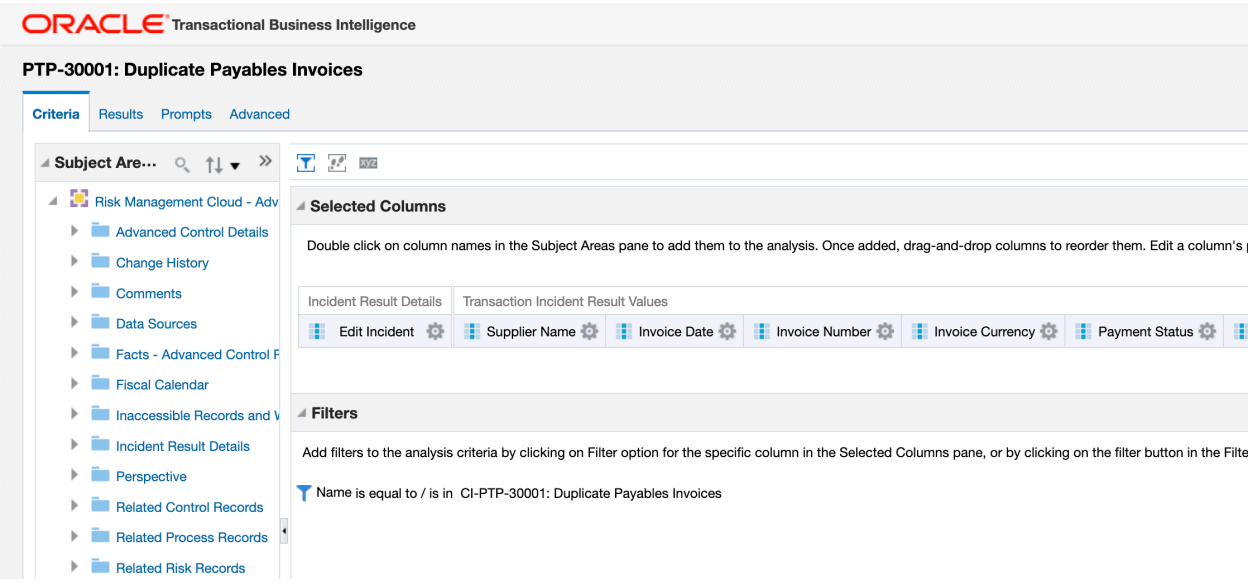
Subsequent steps will show you how to update reports under the '60 Monitor Transactions' folder.



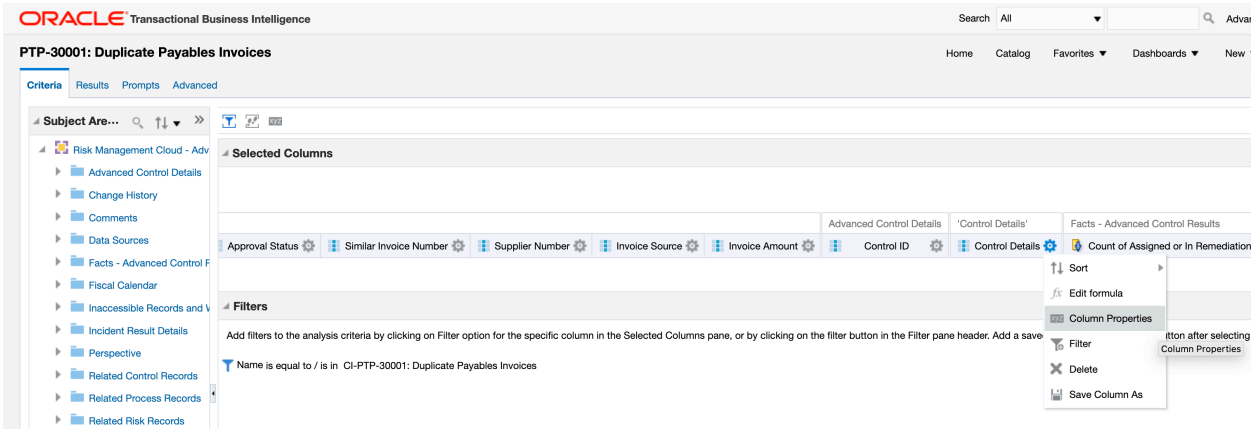
Step 2: Update Each Control Detail Report

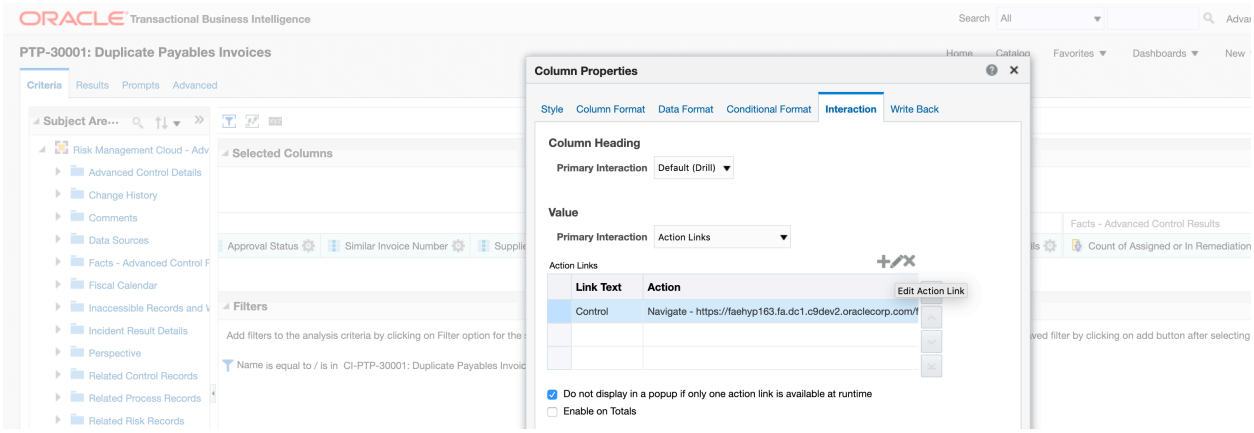
With your Risk Management Dashboard in place, you will need to update URL deep links with the host/environment name for reports under folder '60 Monitor Transactions'. In the following example, the URL name will use development environment called: *faehyp163.fa.dc1.c9dev2.oraclecorp.com*.

Start by selecting Edit for report "PTP-30001: Duplicate Payables Invoices", and go to the Criteria page.



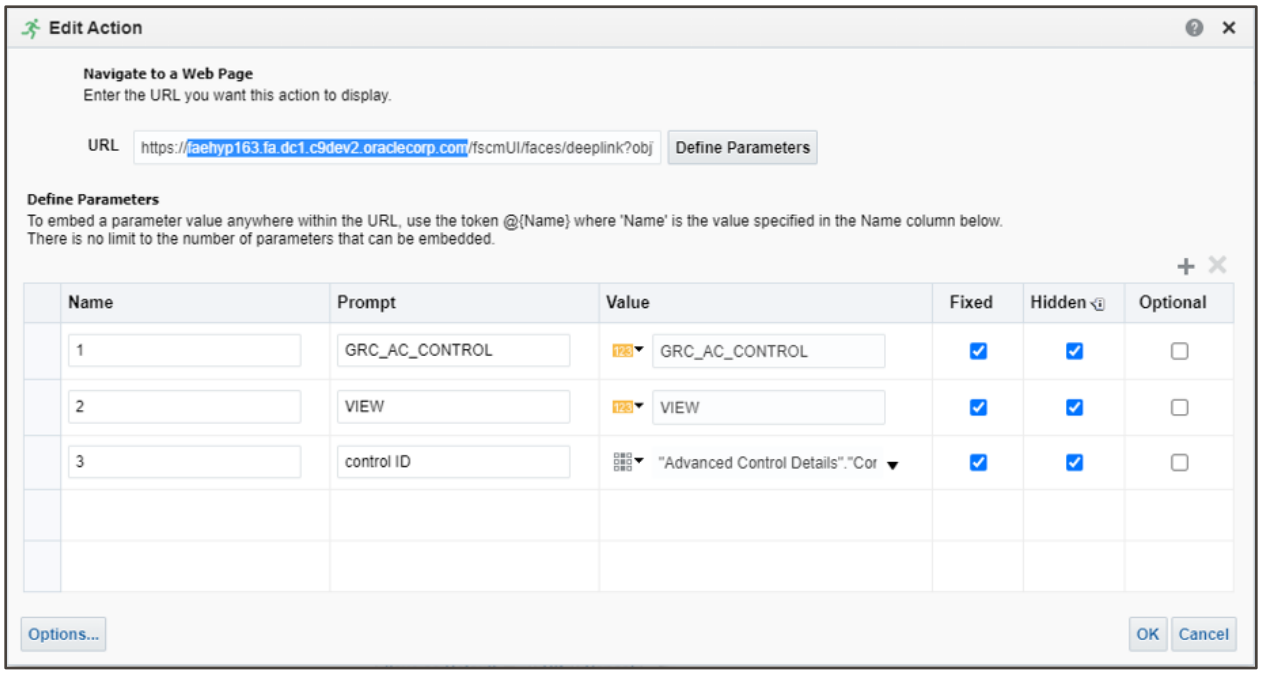
For the ‘Control Details’ column, select the gear box icon then Interaction tab. Highlight the Action Link for control on tab, Edit icon, and Edit Action.



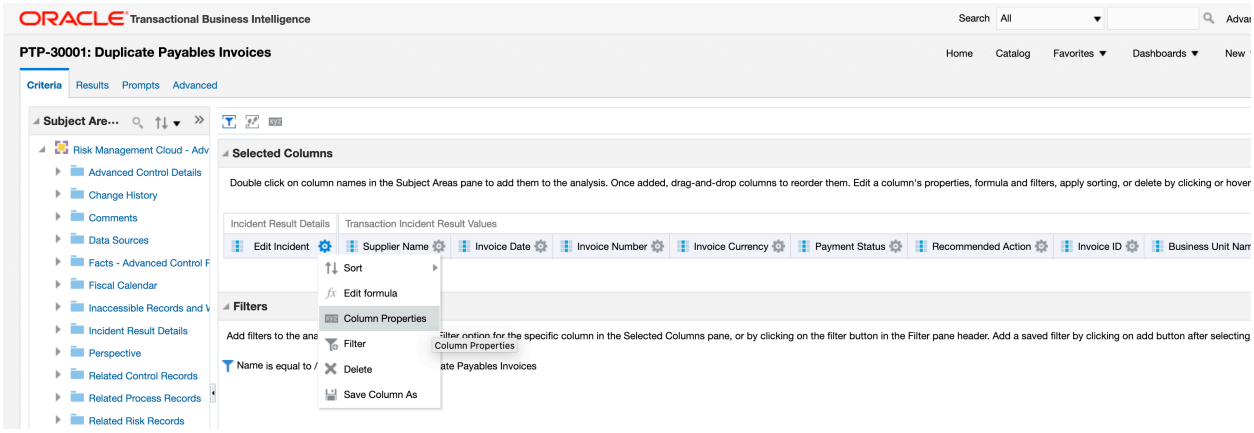


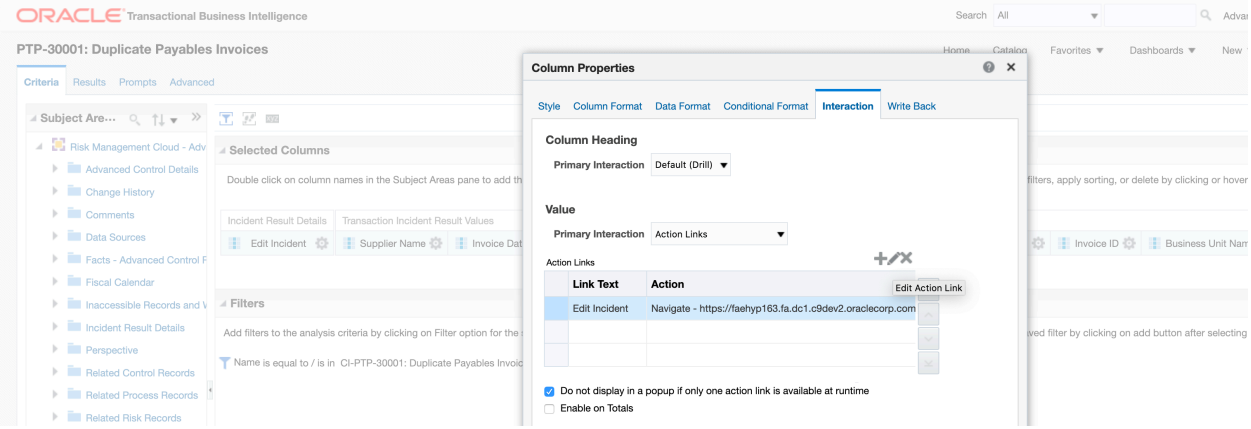
On the Edit Action page, update the URL host name that corresponds to your development environment (see the highlighted section in URL below).

After applying your URL host name, select the OK buttons to save your column changes.



In addition to this ‘Control Details’ column, apply the exact same Edit Actions and URL changes to the ‘Edit Incident’ column. Save the report changes (save icon in top, right-hand corner of page) and return to the catalog folder ‘60 Monitor Transactions’.



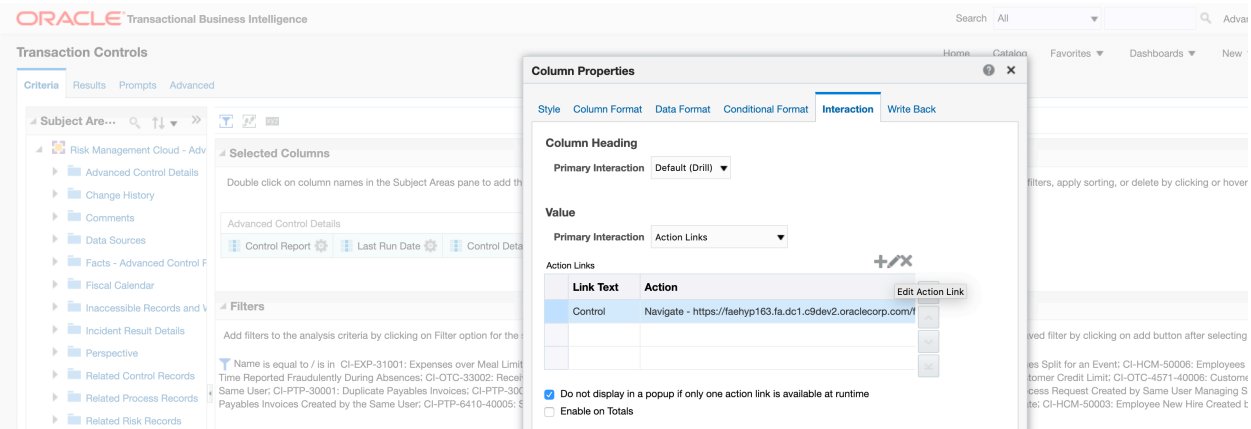


Perform the same steps for the remaining controls' reports in this folder, updating the URL for deep links for 'Control Details' and 'Edit Incident' columns.

Important: The control reports and the column details in OTBI for 'Transaction Incident Results Values' dimensions correspond to attributes, or any calculated column like counts, from the control. This blueprint assumes no changes have been made to the delivered models. Any attributes or model logic changes to delivered models will affect alignment to OTBI report columns defined under folder'60 Monitor Transactions'.

Step 3: Update Transaction Controls Report

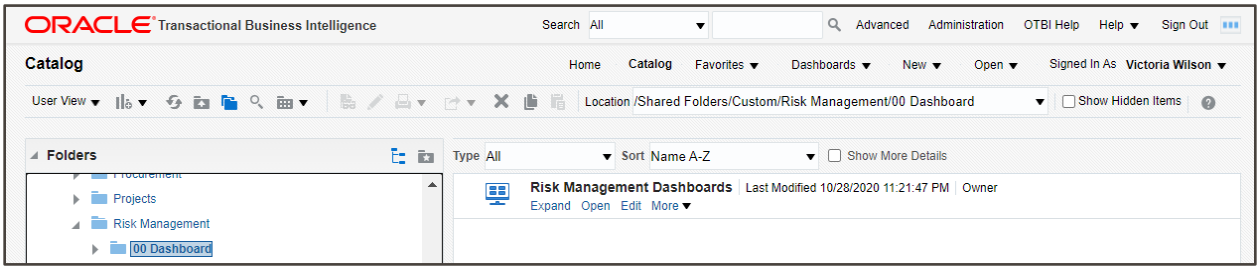
Similar to prior steps for control detail reports, the "Transaction Controls" report used in the dashboard also requires updating to columns using your environment URL host for deep links. Edit the action links for 'Control Details' and 'Pending Incidents' columns, just as described in the previous step. Save the report and return to the '60 Monitor Transactions' catalog folder.



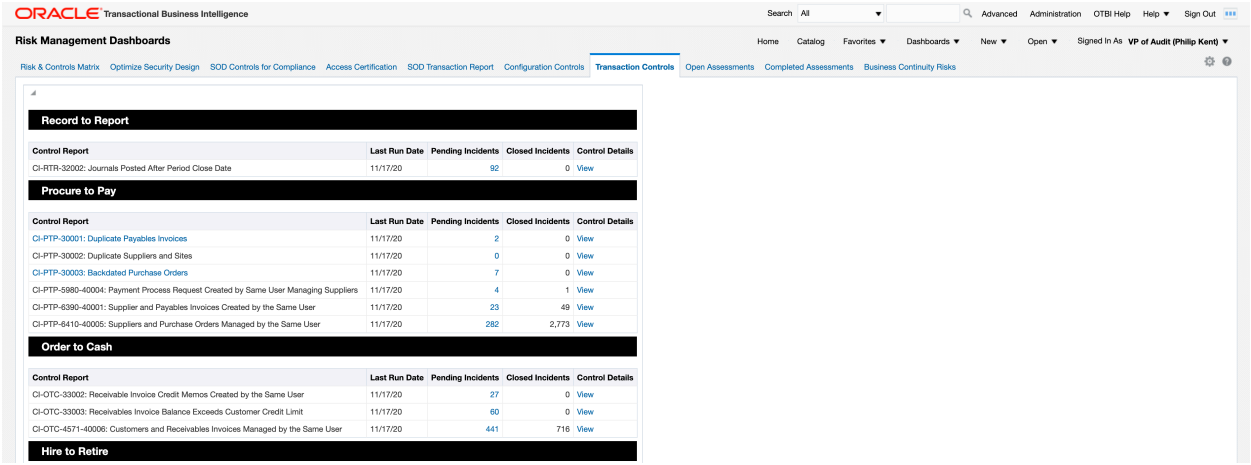
Note: A deep drill on the Closed Incidents column is not currently supported.

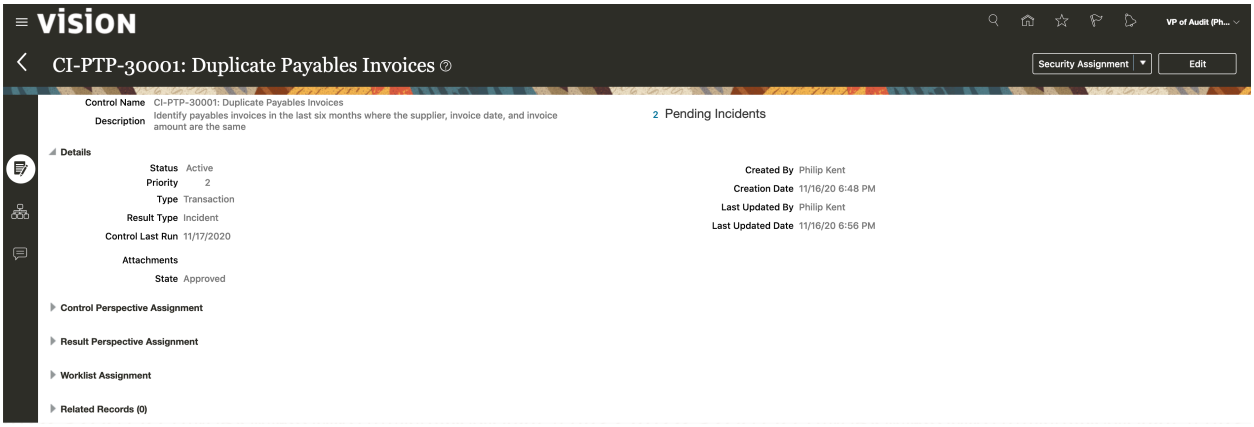
Step 4: Validate Risk Management Dashboard

To test the updates made to URL deep links, Open the Risk Management Dashboards under the '00 Dashboard' folder.

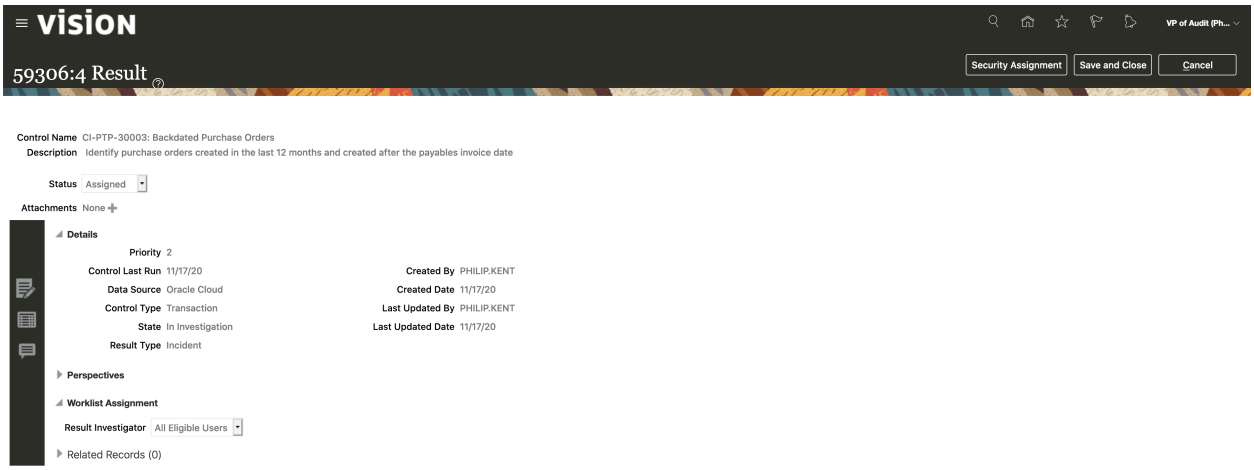


Go to the Transaction Controls page in dashboard to review reports. Test each of the Control Report links to confirm the corresponding OTBI reports are as expected. Additionally, verify links to Pending Incidents and Control Details that open a new window to Risk Management.





Finally, within each control report, there is an Edit Incident link where you confirm it opens a new page for the specific Result ID in Risk Management.



Important: As part of the process defined in this blueprint, the only changes made to the delivered models from the Advanced Audit Controls library are updates to the model/control name to prefix it with something like "PTP-". This has a direct impact on using the Transaction Controls dashboard (organized by business process) delivered on Customer Connect.

Evaluating and Closing Incident Results

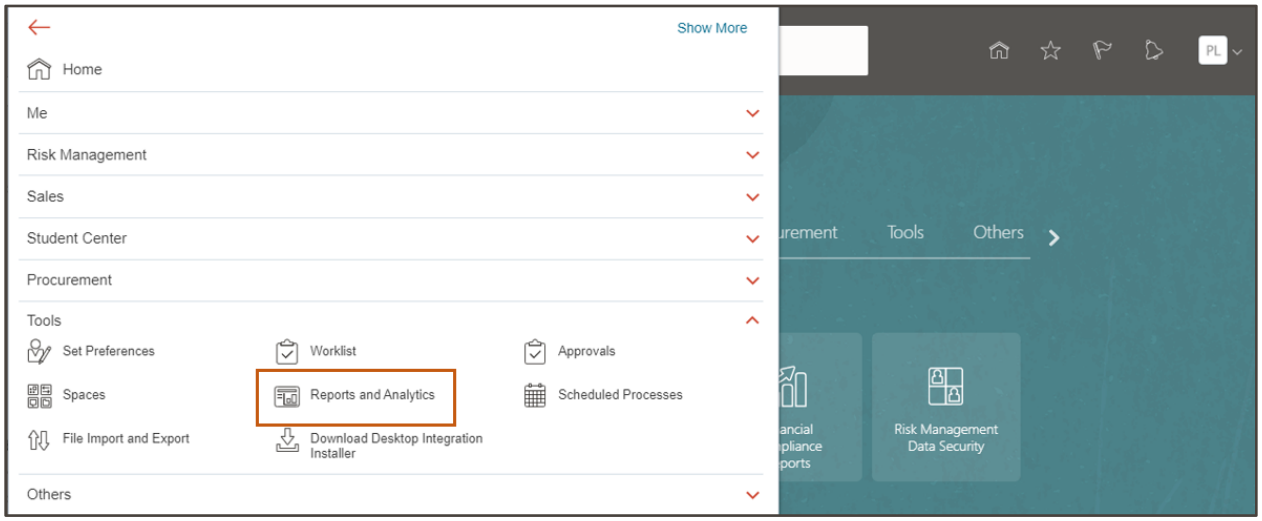
Overview and Participants

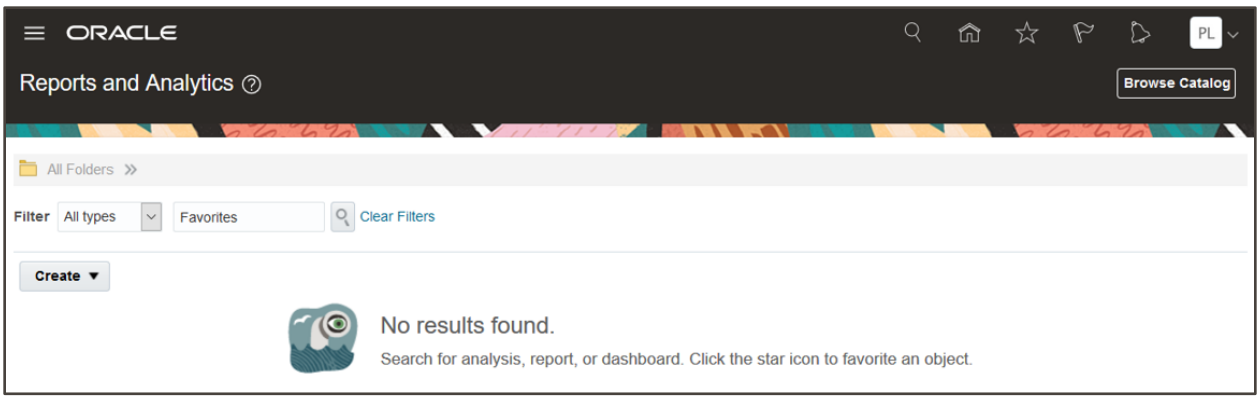
Your risk and compliance team supports business process owners in their review of controls and remediation of incidents. If additional users or security updates are required, they will work with the security team.

Your ERP business process owners will be responsible for validating transaction controls and the incidents they return. They typically are the ones signing off on controls to promote to production, and confirming security assignment responsibility related to these areas.

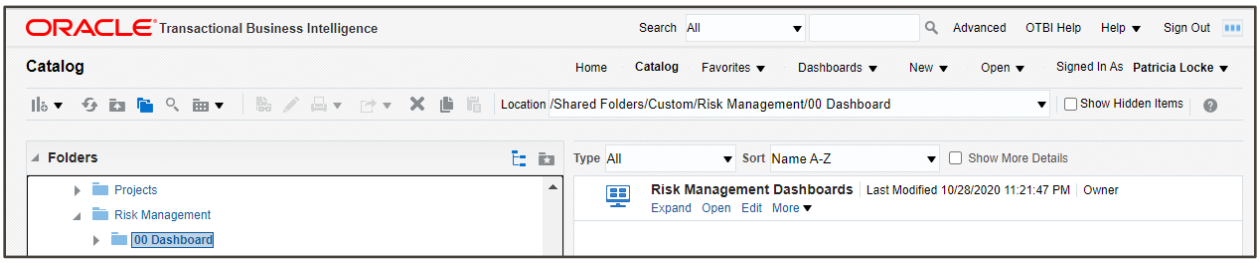
Step 1: Review Risk Management Dashboard

Business process owners will start their review of controls and related incidents from the Risk Management Dashboards in OTBI. Navigate to Reports and Analytics and select Browse Catalog.

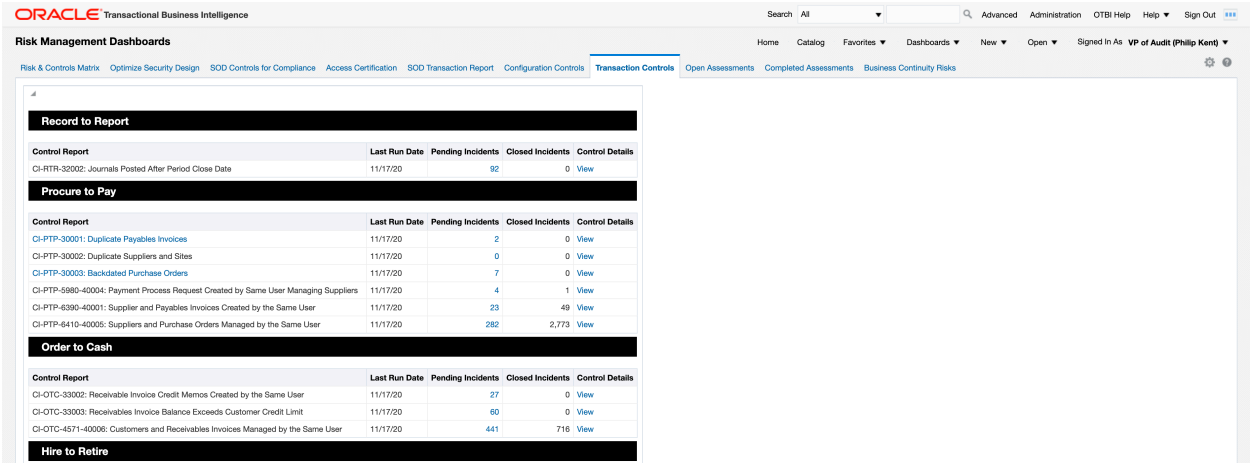




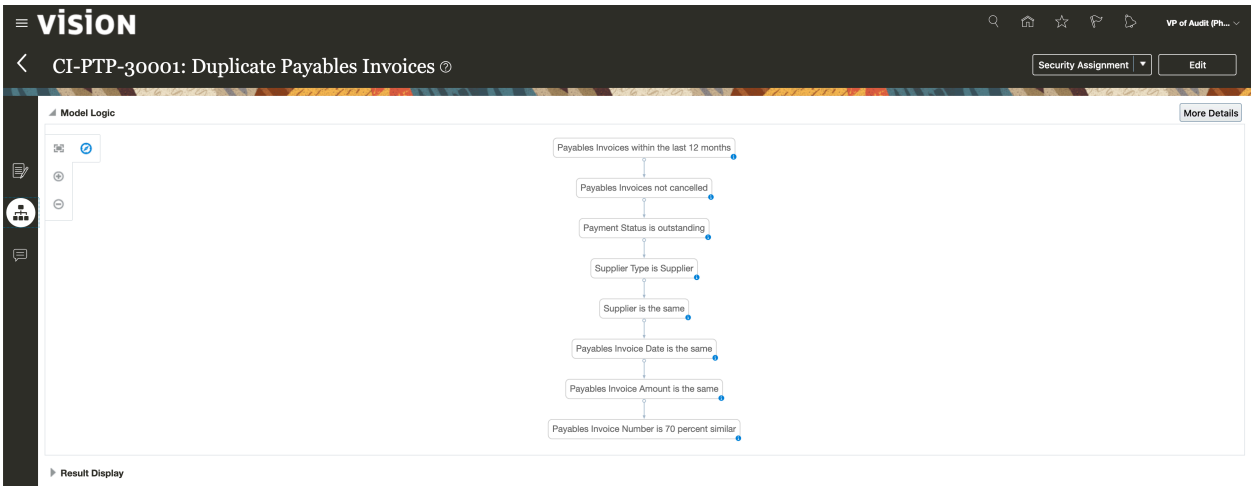
Go to folder Shared Folders > Custom > Risk Management > 00 Dashboard folder, and Open the Risk Management Dashboards.



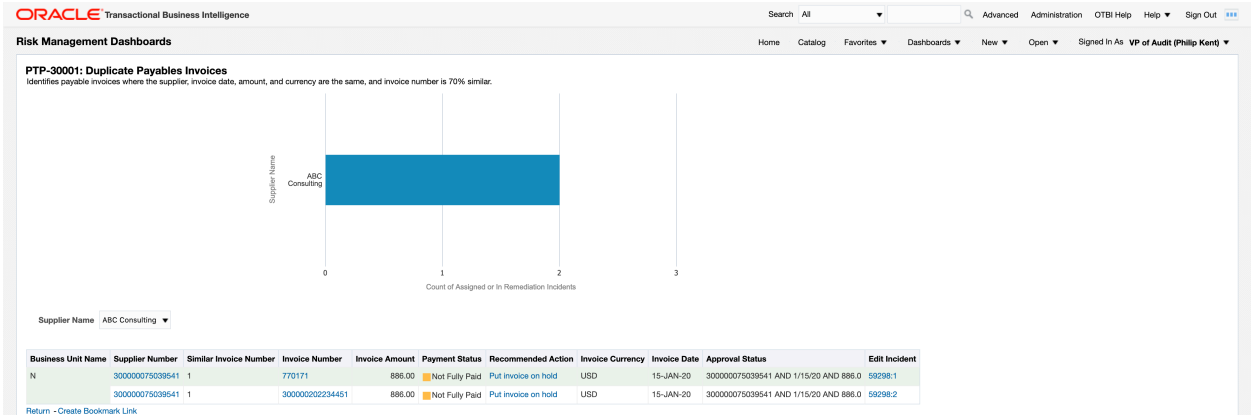
Select the Transaction Controls page in dashboard to review reports. This business user has access to the procure-to-pay control reports, and corresponding incidents and control details.



To review the logic of the control, select the View link under Control Details. A new window to Risk Management opens and you can review the rules that generate incident results.



Access the incident report details by selecting the Control Report name. Here is an example of the report for 30001:

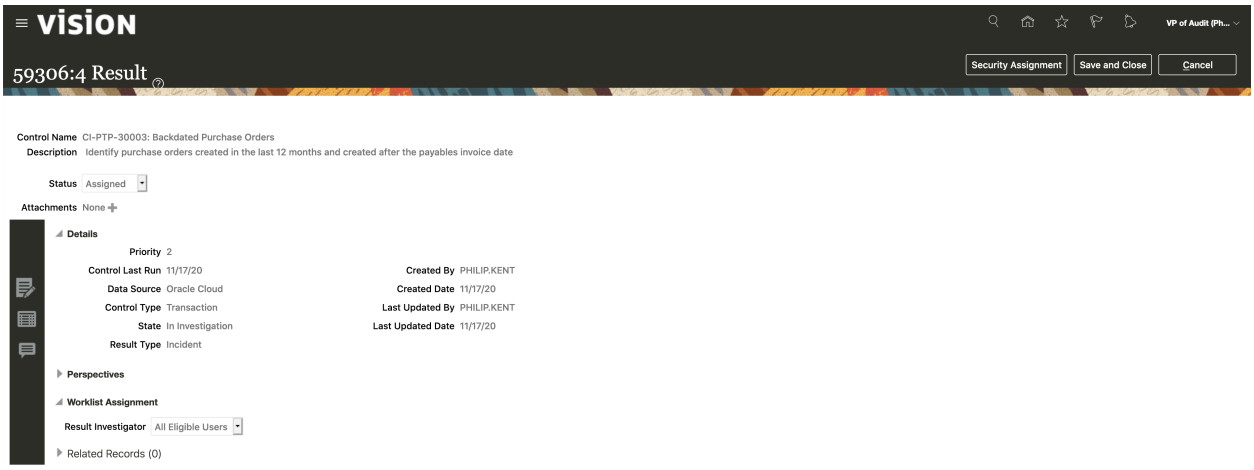


Each control report will vary, and corresponding incident results can be investigated and updated individually or in mass.

Step 2: Edit an Incident Result

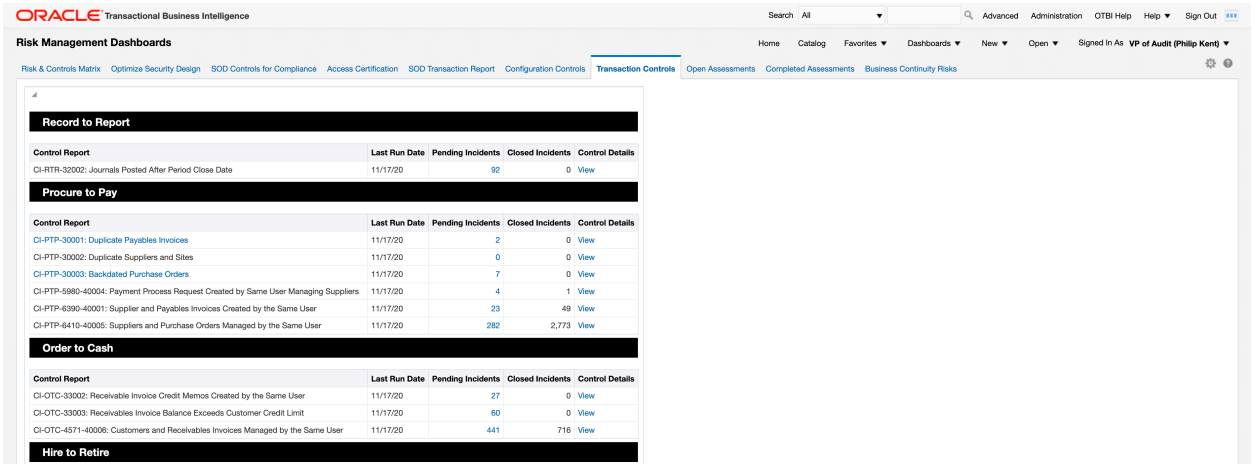
In each of the control report details, you will find a column called ‘Edit Incident’. Select a link at the row level to update an individual incident result.

Here is an example of opening a Result ID in Risk Management from the report for 30001. A new window is opened for the Result ID and you can directly update the Status, add Attachments or Comments.



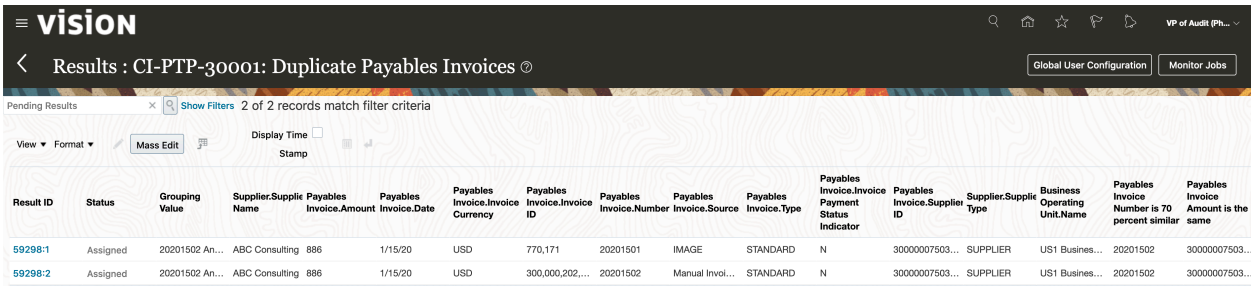
Step 3: Mass Edit Incident Results

Users can also perform a mass update against incident results for a control. To do so, open the Transaction Control dashboard and select the Pending Incidents count to open a new window in Risk Management.

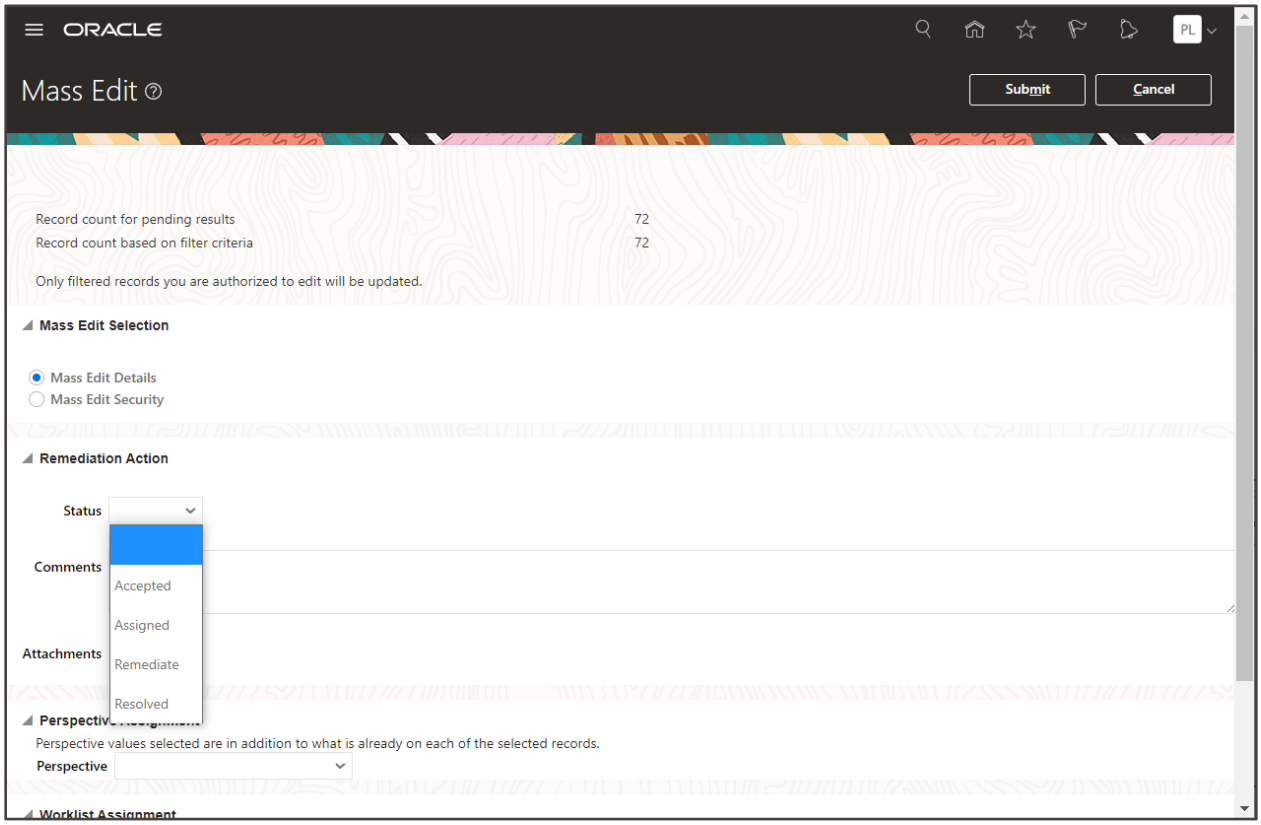


The Pending Incidents are returned for the control selected. Optionally, you can apply additional filters by applying criteria after opening Show Filters.

To apply an update across incidents, select Mass Edit in the page toolbar; it applies to all records in the current view.



The user can mass update the incident details such as status, attachment, and comments, or alternatively update security assignment.



Step 4: Update Risk Management Dashboards

After business process users have tested and made updates to incident result records and their status, those changes need to be updated in OTBI reports and dashboards. A risk administrator will need to run Report Synchronization to update the underlying data presented in the dashboard. Refer to an earlier step for this job - Step 4: Run Report Synchronization.

IMPLEMENT CONTROLS IN PRODUCTION

Summary

Once your business process owners are satisfied with the controls, you are ready to promote them to production. Perform the same steps you applied in the development environment into production, including any prerequisites, with one exception: do not apply test data!

Other Activities

Scheduling

You should place key jobs in production on a schedule, such as:

- Data Synchronization under Advanced Controls Configurations
- Security Synchronization on Scheduling tab under Setup and Administration
- Report Synchronization on Scheduling tab under Setup and Administration
- Control analysis (one or many), Schedule from action toolbar on the Advanced Control > Controls tab

Incident Status

Communicate a status treatment across incidents with business process users. It is intended to use the following delivered status options in the following situations:

- Accepted - means you have determined that nothing needs to be done to resolve the incident.
- Remediate - means you have decided that some action must be taken to resolve the incident.
- Resolved - means you have confirmed that the remedial action has been carried out.

Notifications

When you deploy your controls to production, refer back to optional Step 7: Enable Email Alerts. You need to enable Email notifications if you want to notify business process users that new control incidents require their attention.

Note: Notification jobs are embedded in the 'Security Synchronization' job when new incidents are created and sends out bell messages and optional emails to result investigators. This job was covered in Step 6: Run the Security Synchronization Job.

Security Updates

Any authorization updates in Risk Management after models and controls are deployed in production, a risk administrator can perform Mass Edit Security Assignment under the Risk Management Data Security icon.

ONGOING USE

Over time you will accumulate transaction data. One of the simplest ways to keep syncs and analyses running fast, and avoid being overwhelmed by old data that is no longer relevant to your analyses, is to change "Transactions Created as Of" to a more recent date (see "Step 4: Configure Advanced Controls" above).

BEST PRACTICE CONTENT LIBRARY

This document has shown how to configure key controls – there are many more ERP Advanced Transaction Controls models that you can use by following the same instructions.

RELATED RESOURCES

Solution Blueprint Dashboards and Reports
https://cloudcustomerconnect.oracle.com/posts/6ac0498b5e

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

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

Oracle Risk Management Cloud Documentation for 21A
https://docs.oracle.com/en/cloud/saas/risk-management/21a/books.html

Key guides here include:

- Using Advanced Controls
- Implementing Risk Management
- Securing Risk Management
- Security Reference for Risk Management