ORACLE

Continuously Monitor Configuration Changes

Step-by-step guide

February 2021 | Version 1.0
Copyright © 2021, Oracle and/or its affiliates

SUMMARY

Oracle Cloud ERP lets you monitor changes to configurations of business processes such as procure-to-pay and general ledger, using Audit Policies. When you configure those policies for specific ERP business objects and attributes, you continuously monitor create, update, and/or delete actions (events) and the values involved. While that continuous monitoring is valuable, it requires manual analysis of changes and manual initiation and management of responses.

Oracle Risk Management automates those activities by providing advanced analyses that raise visibility of anomalous and unwanted events that might otherwise go undetected, and workflows that orchestrate and track your organization's responses. It also joins those activities with automated analysis of user security configurations for holistic control over what users can do, and of the transactions created and approved by those users, for mitigating control when configurations must allow risky activities; and the related response and governance workflows.

This document provides you a guided process to configure, import, test and verify some key configuration monitoring controls. Its step-by-step instructions help you:

- Configure change tracking to help coordinate risk management activities across your organization
- Quickly deploy pre-built library of best-practice controls for configuration changes
- Continuously monitor changes to detect any fraudulent activities
- Investigate changes using dashboard reports

DEVELOP MODELS & CONTROLS IN A NON-PRODUCTION ENVIRONMENT

Audit Considerations

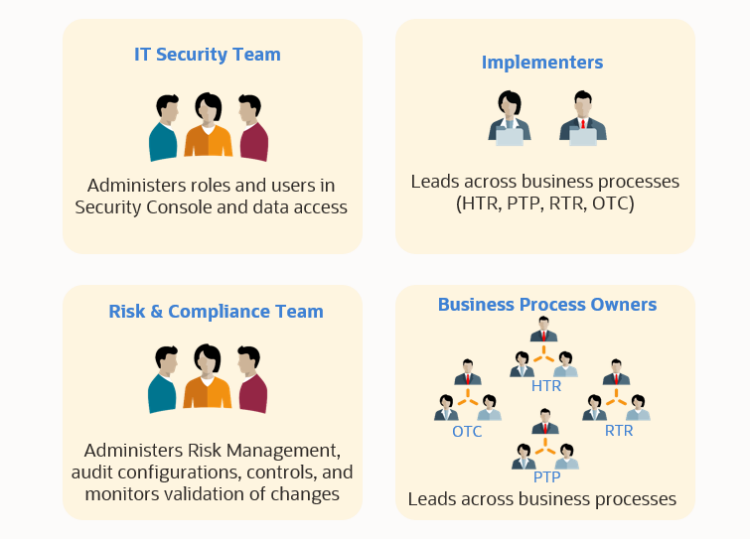
The initial step in any implementation is to decide what you want to end up with. In this case, that starts with identifying the users of the Cloud ERP applications, how they interact with the applications, and what configurations will be monitored. For example, are there business process owners who rely on the application configurations, or an internal audit team who needs to make sure that expected configuration settings are in place and monitored regularly?

Before you follow the steps in this guide, review our documentation on managing Audit Policies for the Cloud ERP applications, securing and implementing Risk Management, and using Advanced Controls – see the Related Resources section of this document. 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 with those guides, and this step-by-step guide, define and secure participant responsibilities across your organization. Consider the answers to the following questions while developing configuration controls to identify the following participants, responsibilities, user groups, and their security access:

- Who will determine what configuration changes to track
- Who has access to configure or modify Audit Policies (such as enabling supplier bank account change tracking)
- Who will monitor and audit the change events identified by the Audit Policies
- Who will review configuration changes and provide supporting documentation
- Who will determine the appropriate remediation action if required
- Who can take action on preventing future change violations

For purposes of this step-by-step guide, 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.

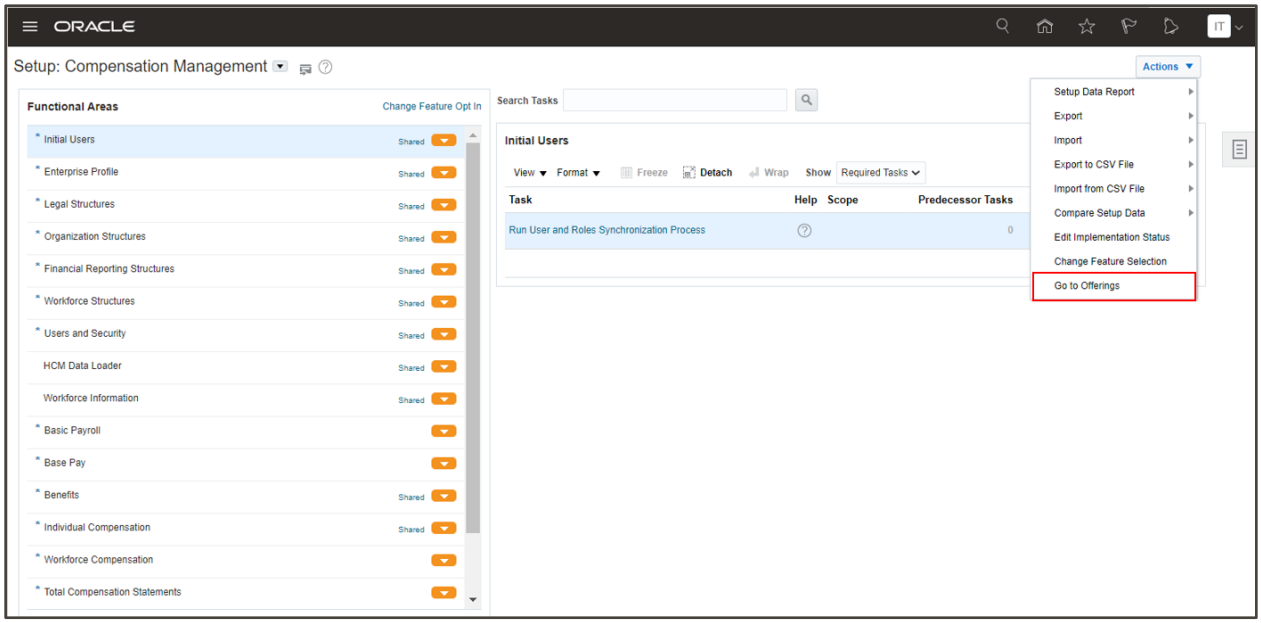
Your security team will grant access to the risk and compliance team to setup Risk Management.

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

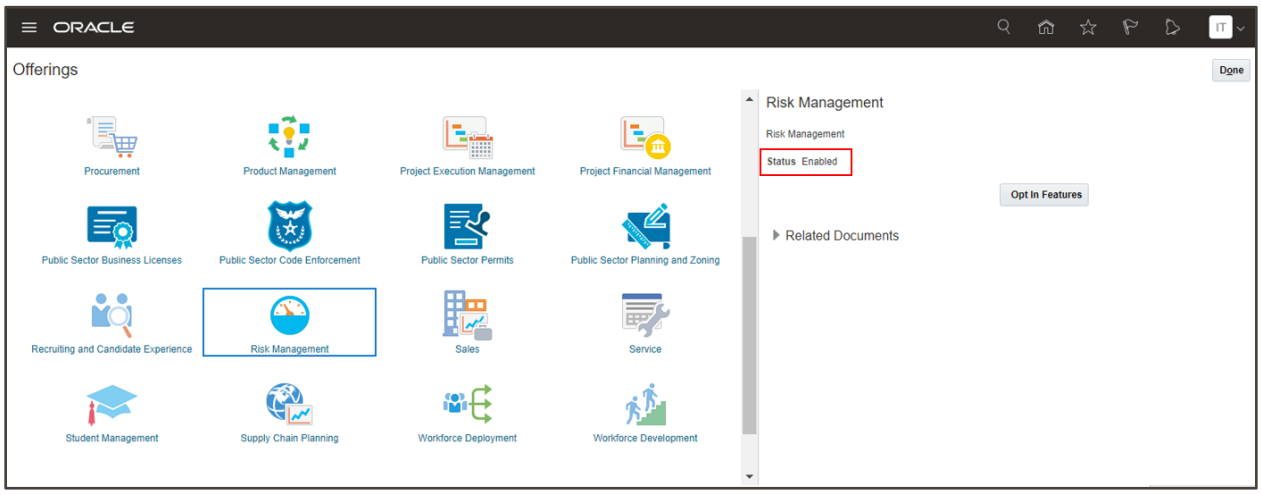
Step 1: Activate Risk Management

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

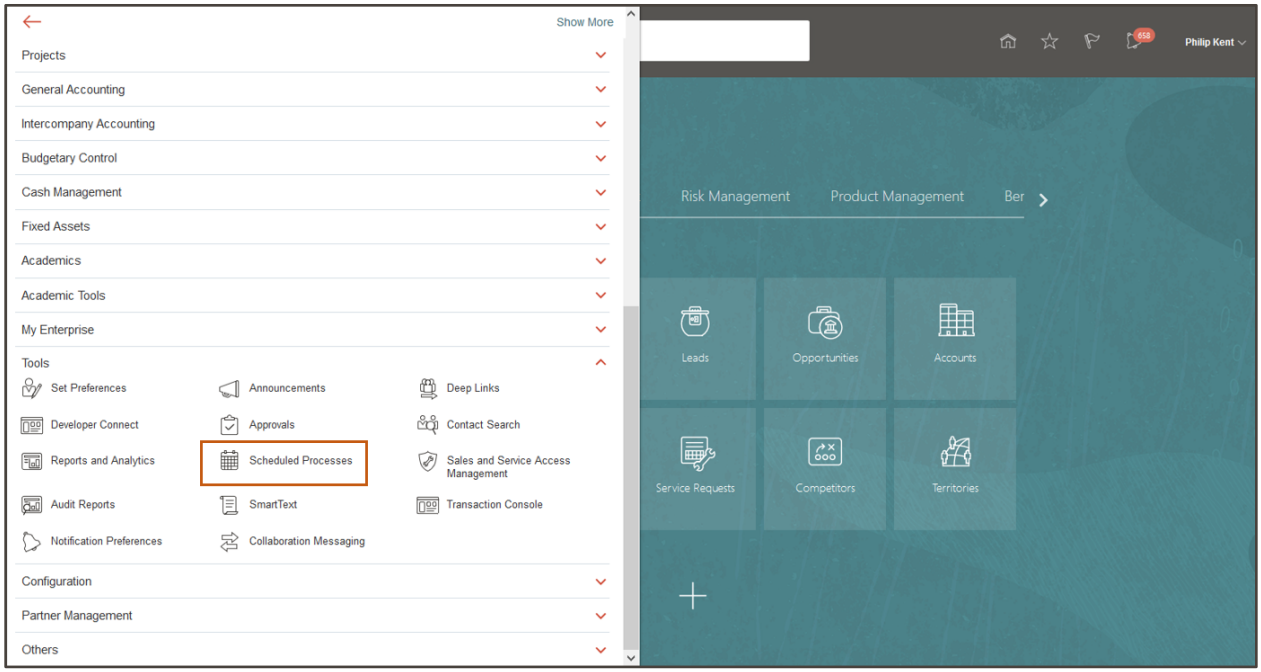
The security team grants user role access through the Security Console. Assign your user security to match their responsibility, whether it is to setup Risk Management, manage Audit Policies, or monitor configuration controls. Depending upon their participation across the processes documented, these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

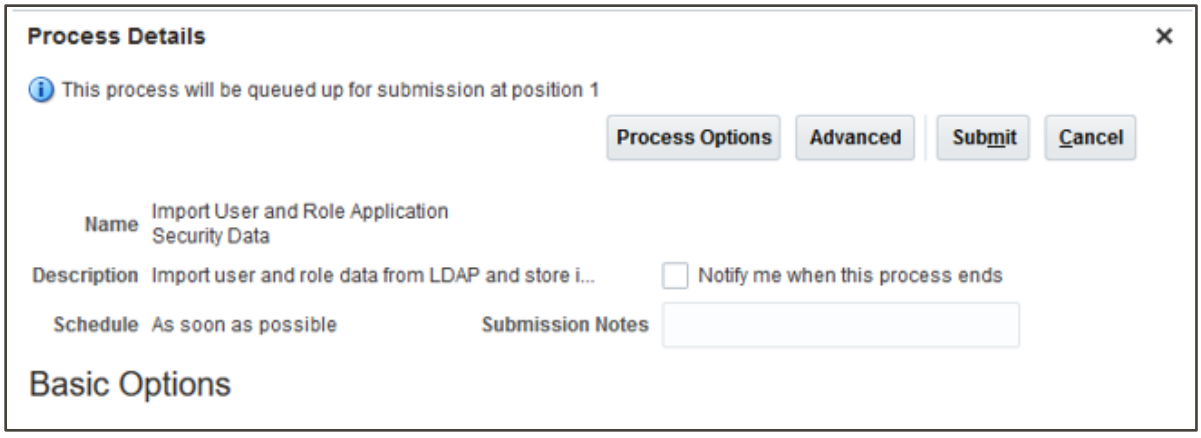
- Risk Administrator
    - Defines business object security, configures performance dates for data synchronization, runs jobs for controls, security, report and data synchronization, and related scheduling.
    - Role code: ORA_GTG_RISK_ADMINISTRATOR_JOB
- Application Implementation Consultant
    - Manages Audit Policies to support configuration controls, reviews audit reports, 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.



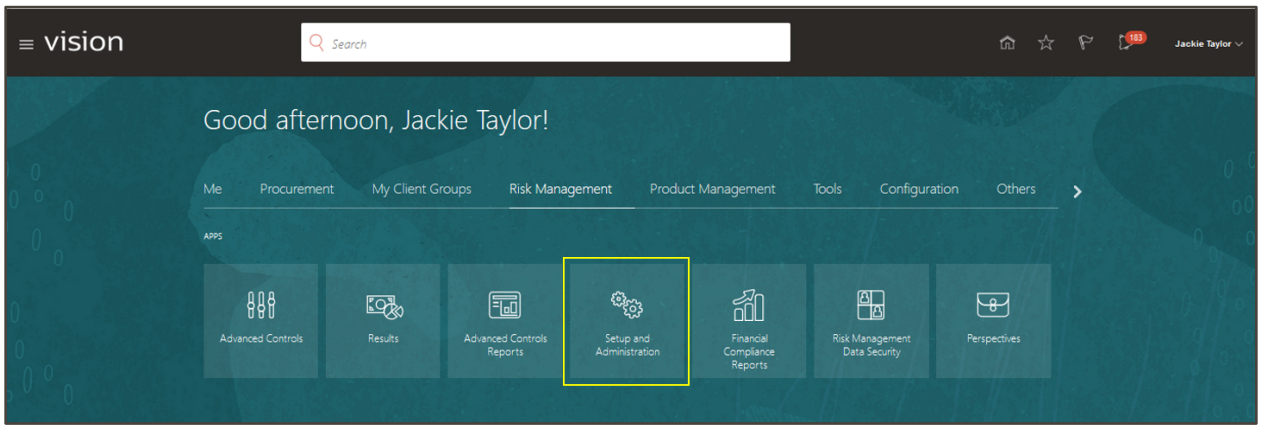


If you need to setup this job on a regular schedule, select the 'Advanced' button instead of Submit to define the schedule.

Step 4: Configure Advanced Controls Configurations

As a risk and compliance administrator, you will need to configure audit performance for advanced controls. For audit-related events, you define a created as-of date as the starting point to return configuration changes used in models and controls. However, keep in mind this starting point goes hand-in-hand with the timing of setting up the application Audit Policies, covered in following Audit Policy Prerequisite Steps section.

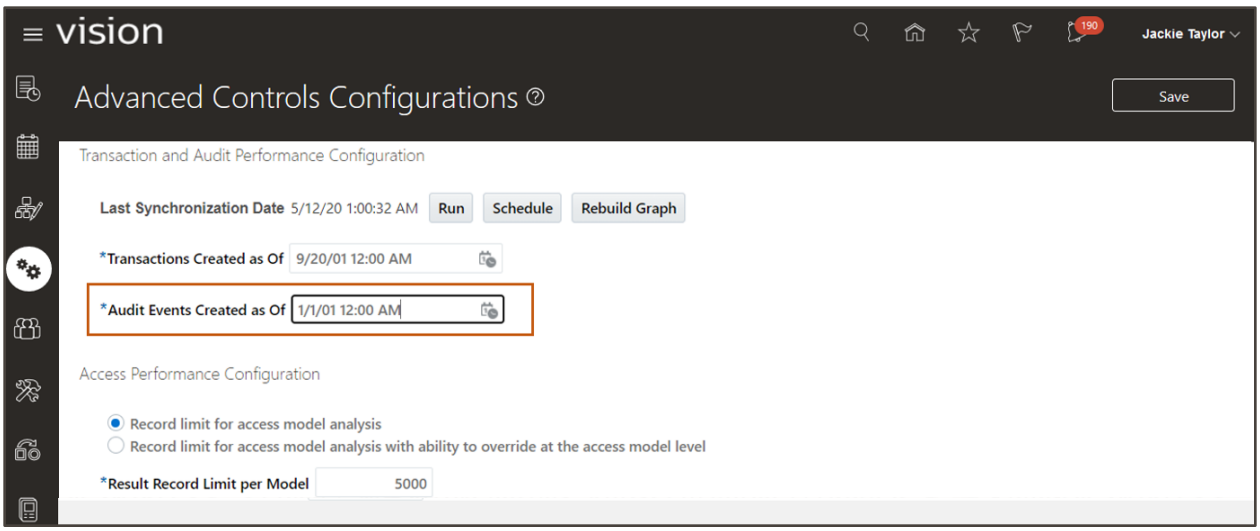
To configure audit controls, navigate to Risk Management > Setup and Administration.



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

- Timeframe business wants to evaluate configuration changes. (This date will most likely be different between development and production environments.)
- Take into account when application Audit Policies are set; your configuration events are only tracked at the time they are added.
- Consider the frequency you will run configuration controls. For example, changes by users are captured at the time saved or approval, but when tracking the number of changes by a business object attribute may occur across several months.
- Note: The Transaction Created as Of date is also a required field, but not used in this document. If this had not previously been set or implemented, for now apply a date as close to current date.

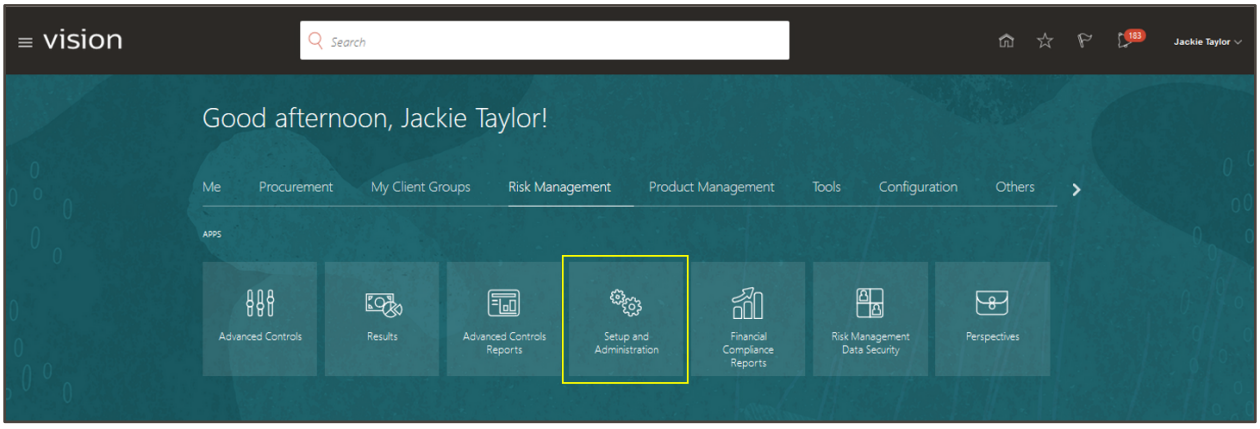
Apply the performance configuration dates and Save the page. No other action is required on the page for configuration controls at this time.



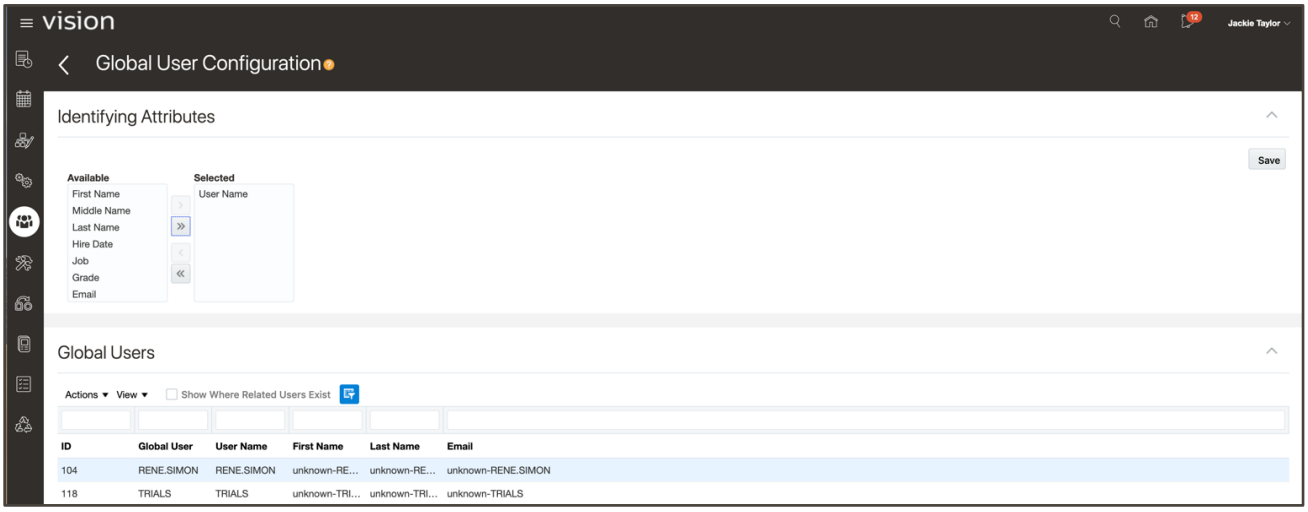
***Note**: Wait to select 'Run' for synchronization until you have imported delivered library content. Synchronization only applies to business objects (BOs) used in a model or control. If it is not used, it will not be synchronized.*

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 and configuration 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.

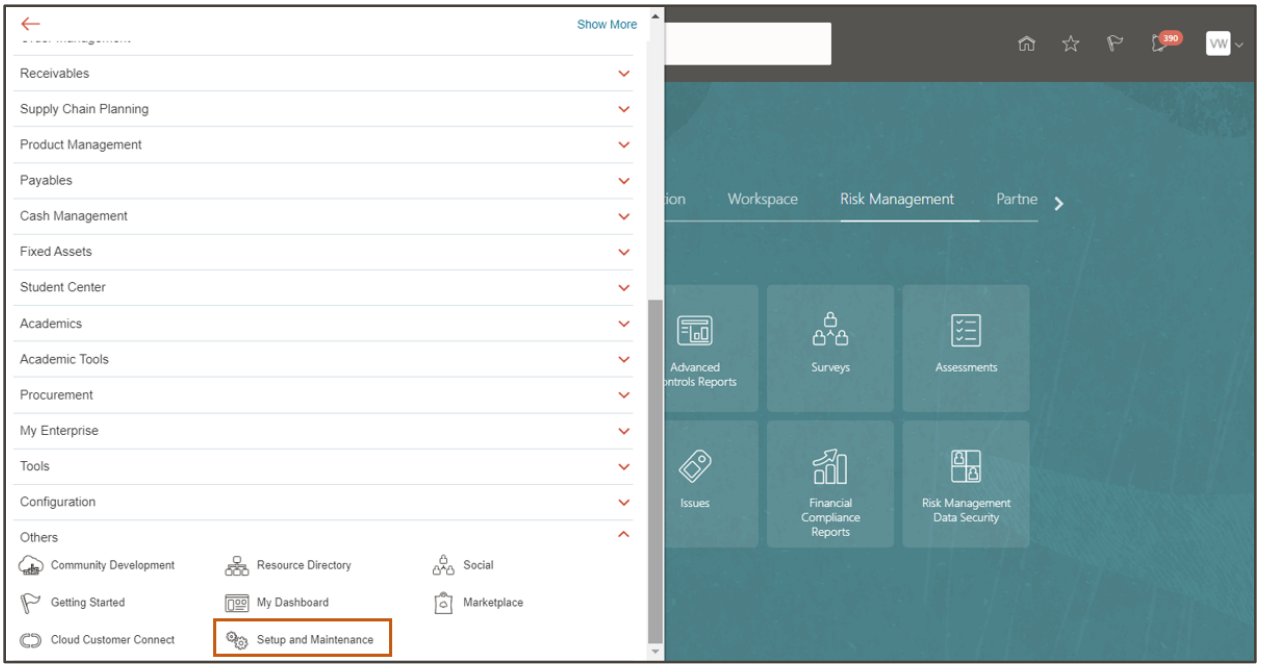
Important: The identifying attributes on the Global User Configuration tab can be changed at any time, but doing so has significant impact. It will purge existing global users, and model results and control incidents that use it. Because of this impact, it is recommended you enable Oracle Cloud auditing for Risks and Controls, which is covered in the following 'Auditing for Risks and Controls' topic.

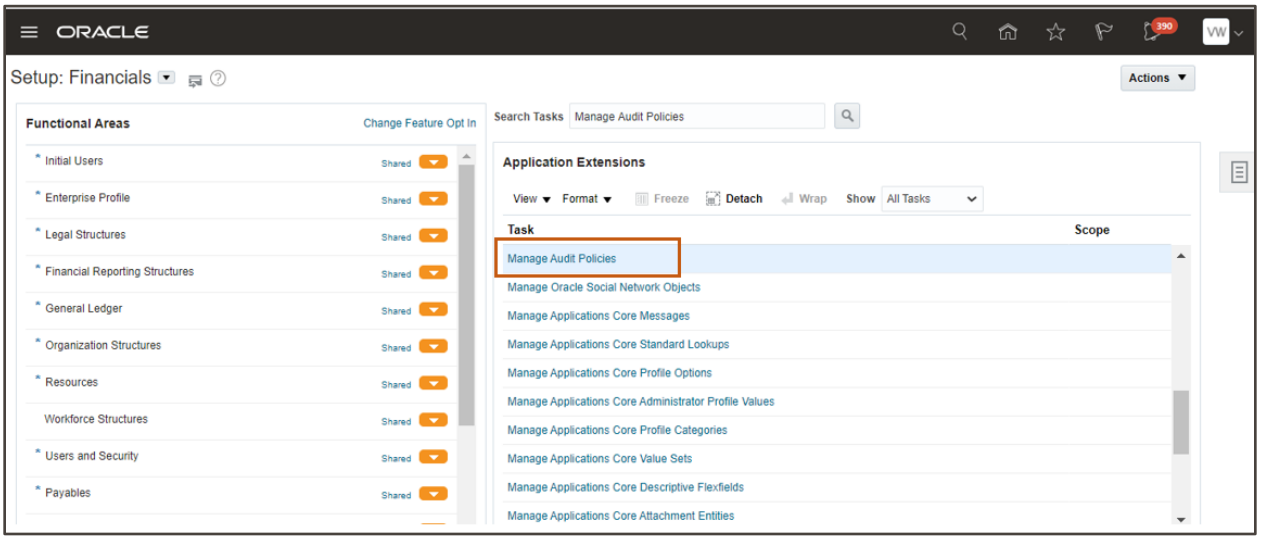
Auditing for Risks and Controls

Configuring Oracle Cloud audit is also covered in detail under the below 'Audit Policy Prerequisite Steps' section, however, that section is specific to the requirements in this blueprint for track change controls in Advanced Controls.

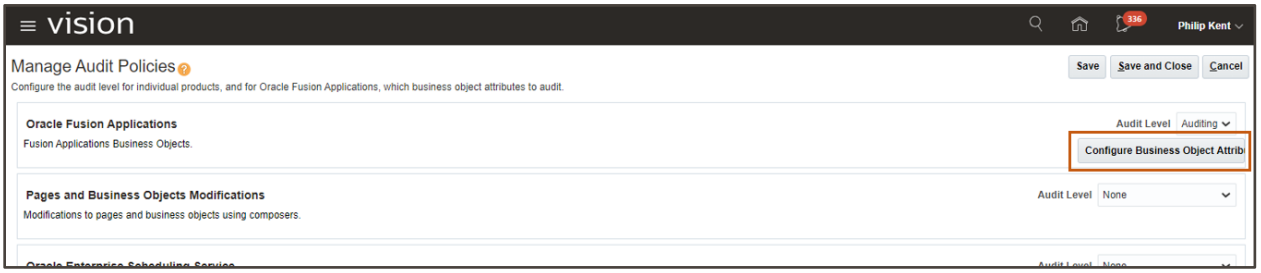
Here, configuring auditing for Risks and Controls is used in the event identifying attributes are ever changed on the Global User Configuration tab, which causes global users and related results and incidents to be purged. The audit information will be helpful in understanding the changes if this occurs.

Navigate to Setup and Administration, and search for the Manage Audit Policies task.



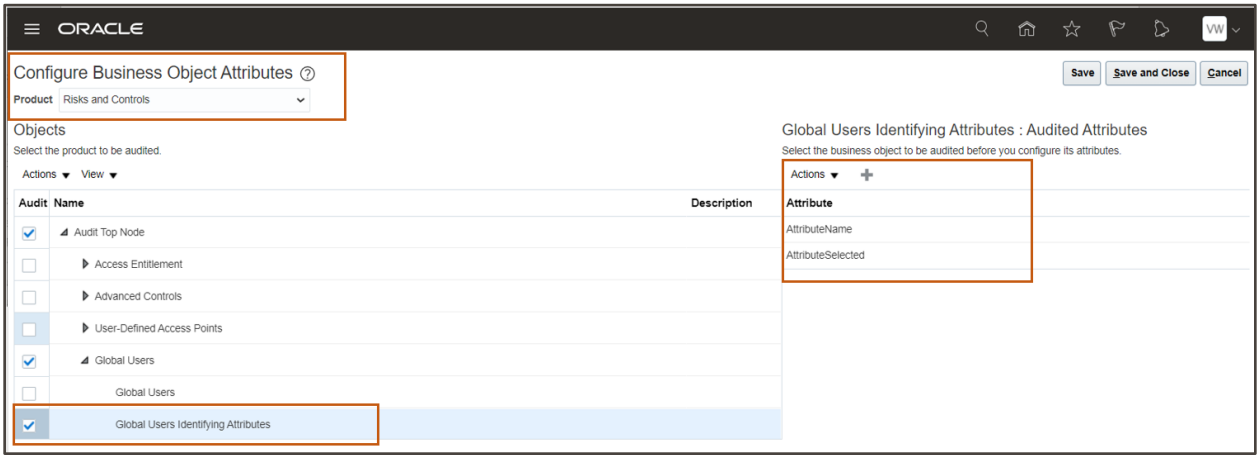


On this Manage Audit Policies page, select the ‘Configure Business Object Attributes’ button across from Oracle Fusion Application.



At the top of the Configure Business Objects Attributes page, select the 'Risks and Controls' Product value from the drop-down.

In the business object table under Global Users, select Global Users Identifying Attributes. To add the attributes to audit, select the + in that right-hand column, or Action > Create, and a popup becomes available to search and add the attributes. Add the AttributeName and AttributeSelected attributes; save and close the configuration page.



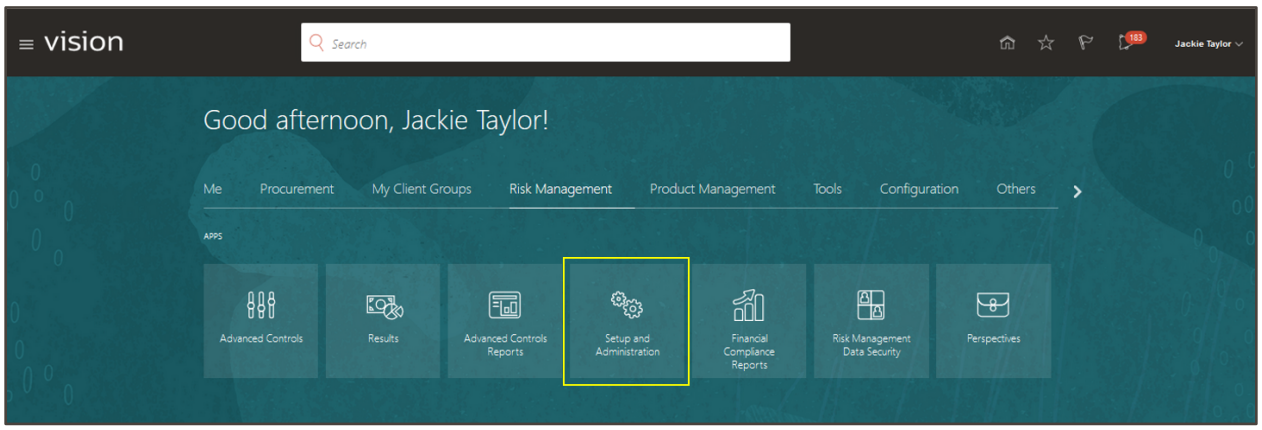
When you select a business object like Global Users Identifying Attributes, you must also select any parent node above the business object to enable the auditing.

Note: In the event there are changes made to the Global User Configuration tab, you can use the Audit Reports tool to review change history. Information on this reporting tool can be found in this document under Audit Policy Prerequisite Steps > Step 6: Review Changes Under Audit Reports.

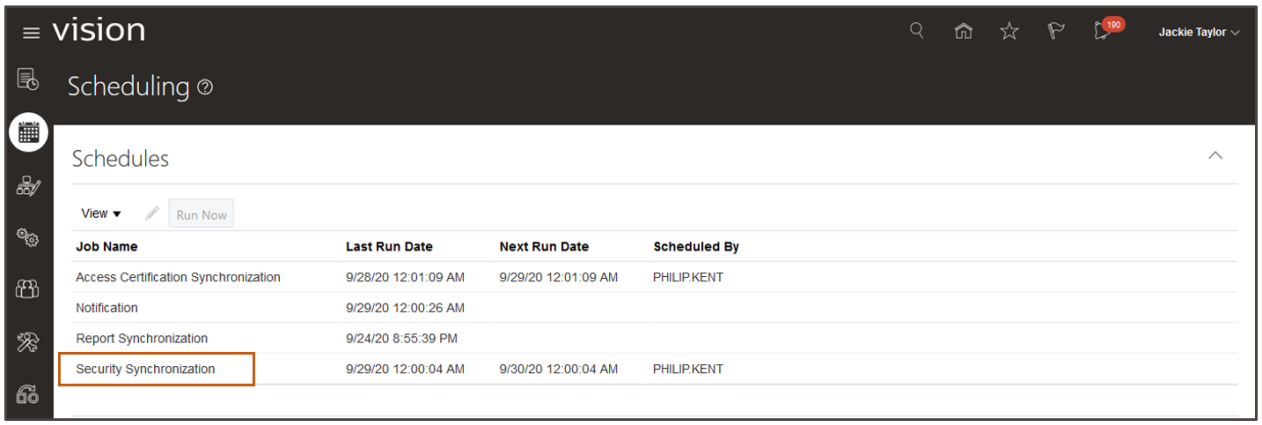
Step 6: Run the Security Synchronization Job

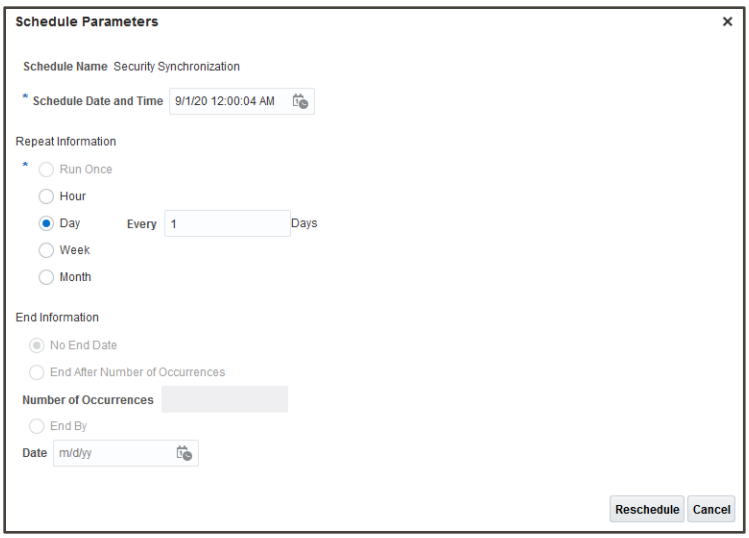
Anytime there are changes made in Security Console, be sure to run the Security Synchronization job, which updates who can access what in Risk Management. The job should be scheduled to run at least daily.

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.



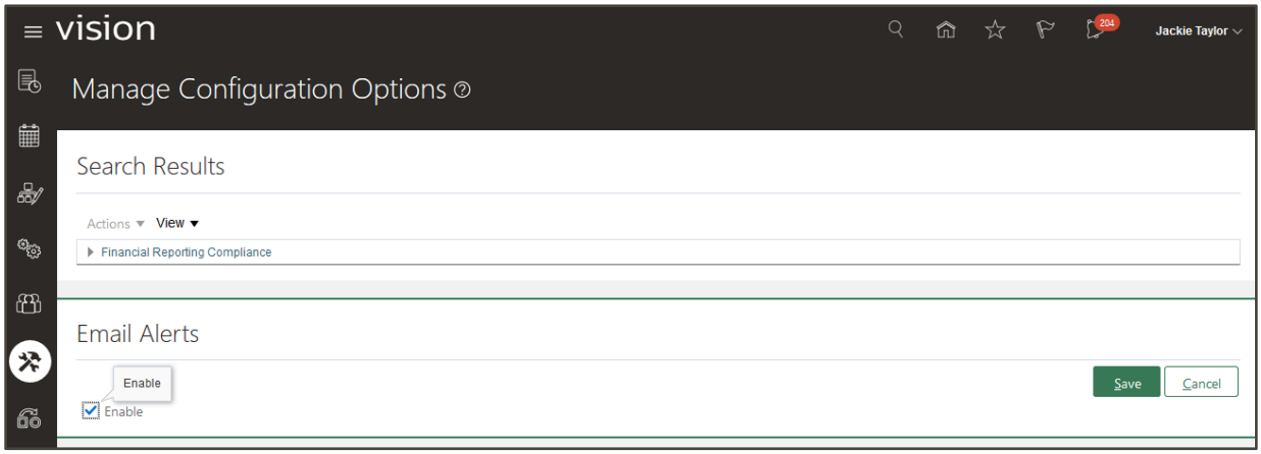


Step 7: Enable Email Alerts (Optional)

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.

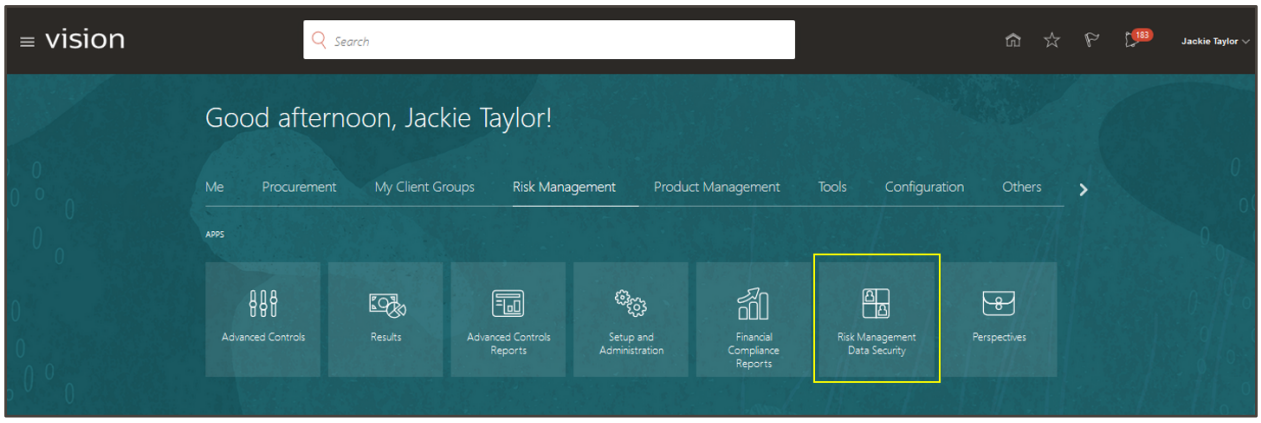
Your risk and compliance administrator will run and create job scheduling in Risk Management to support configuration controls, and maintain related user groups by area.

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 Audit Policies (covered in Audit Policy Prerequisite Steps), but the security team will need to grant data access that functionally aligns to those who will manage configuration models and controls by business area.

There are two ways to define data security in Risk Management, by functional area (such as Supplier Model product) or specific business objects (like Audit – Accounting Period Status). 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.

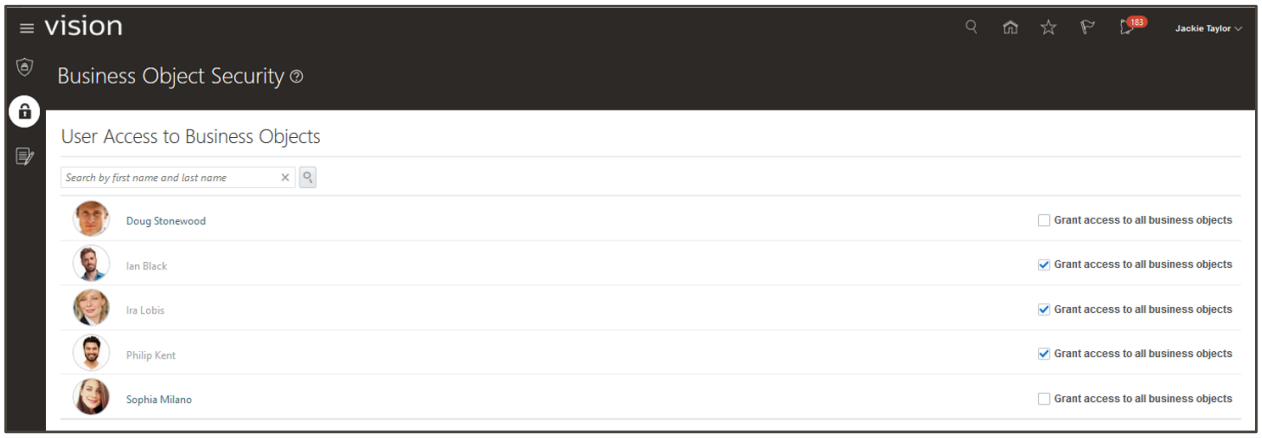


Select the Business Object Security tab.

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.

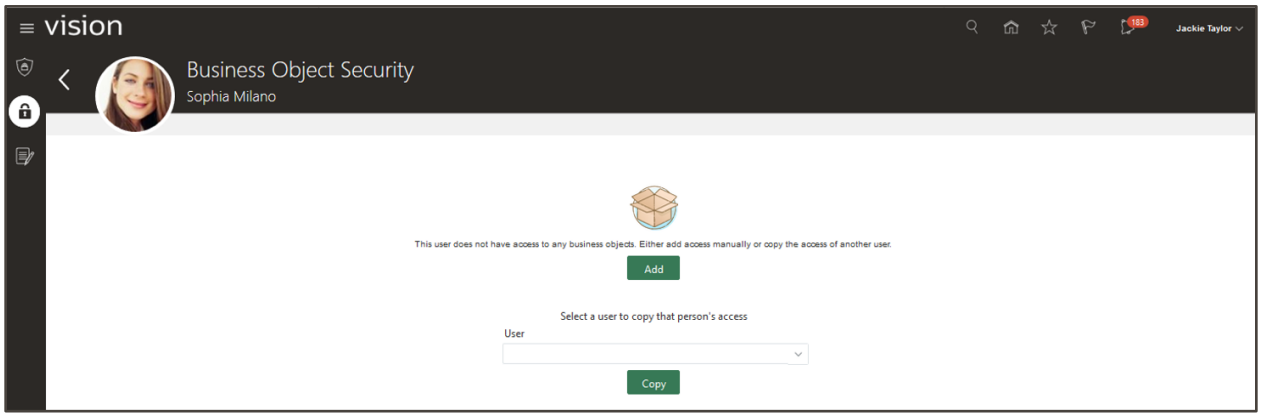
Note: Control incident result access is not dependent on this business object data security, only models and controls.

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.

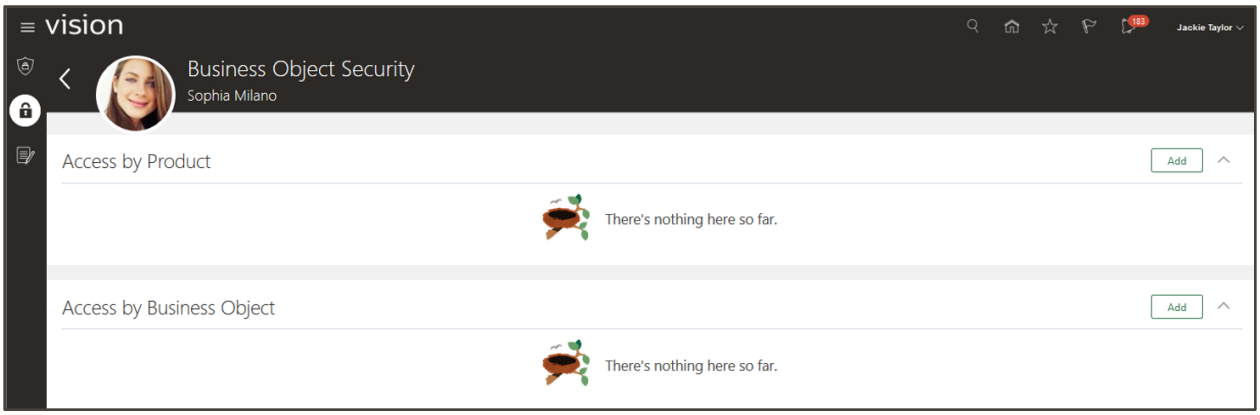


When selecting the user name, a guided process begins, giving you the choice to manually define business object access, or copy another user's data access. This user will be defined to access business objects for changes to supplier configuration, related to procure-to-pay processes.

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

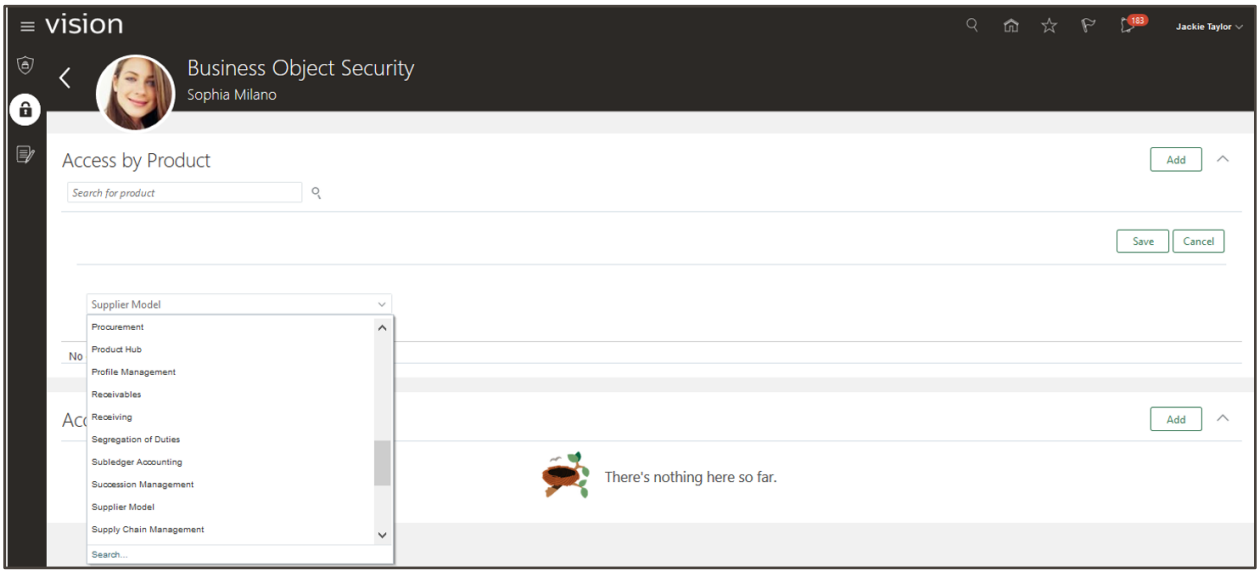


You can define the user's data access by product area or business object. Here in this example, select the Add button for 'Access by Product' region.

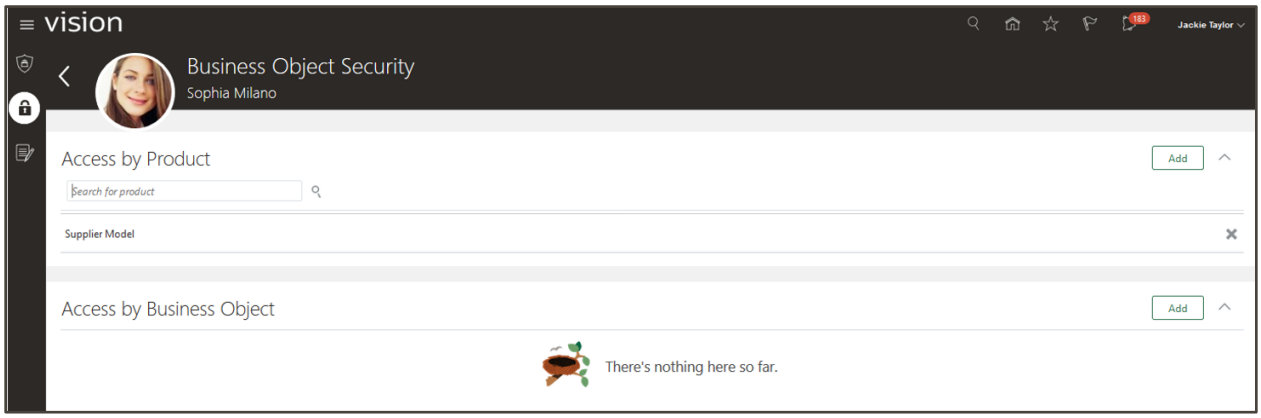


All business objects delivered in Advanced Control are related to a Product name, typically representing a functional area such as Payables Invoice, General Ledger, and Supplier Model. To align with ERP configuration changes related to supplier, select the 'Supplier Model' product area, and Save the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

Several delivered best practice models are associated to this product area for supplier master configurations, such as "60001: New Bank Account Added to Supplier" and "60002: Frequent Changes to Supplier Bank Accounts".

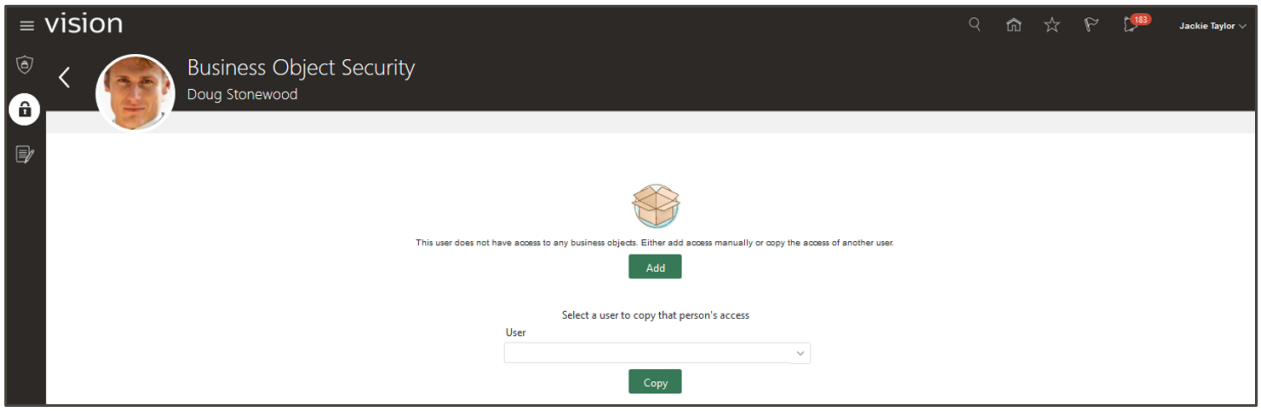


Now you have a user associated to Supplier Model, where they can view, edit, or own models and controls that contain business objects associated to this product area.

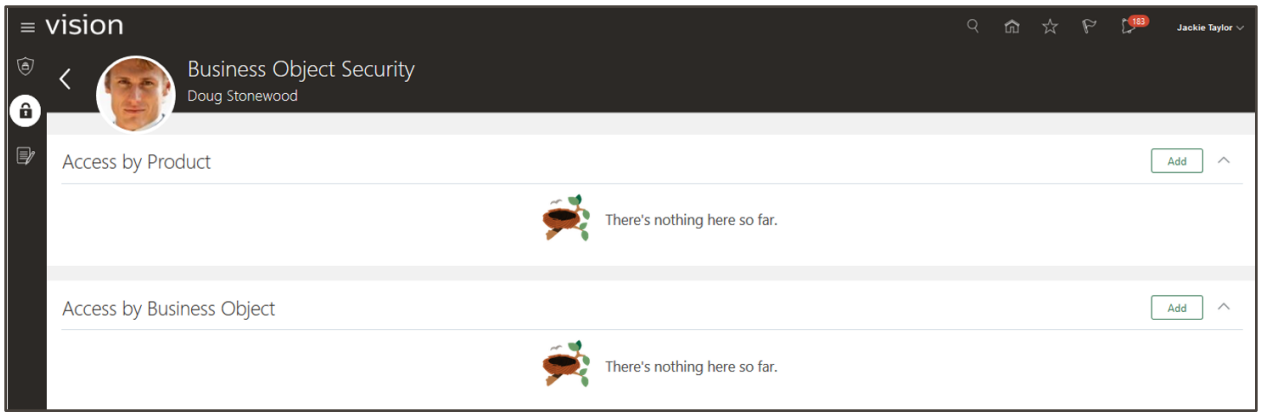


In this next example, let's define a user's access by business object instead of product.

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

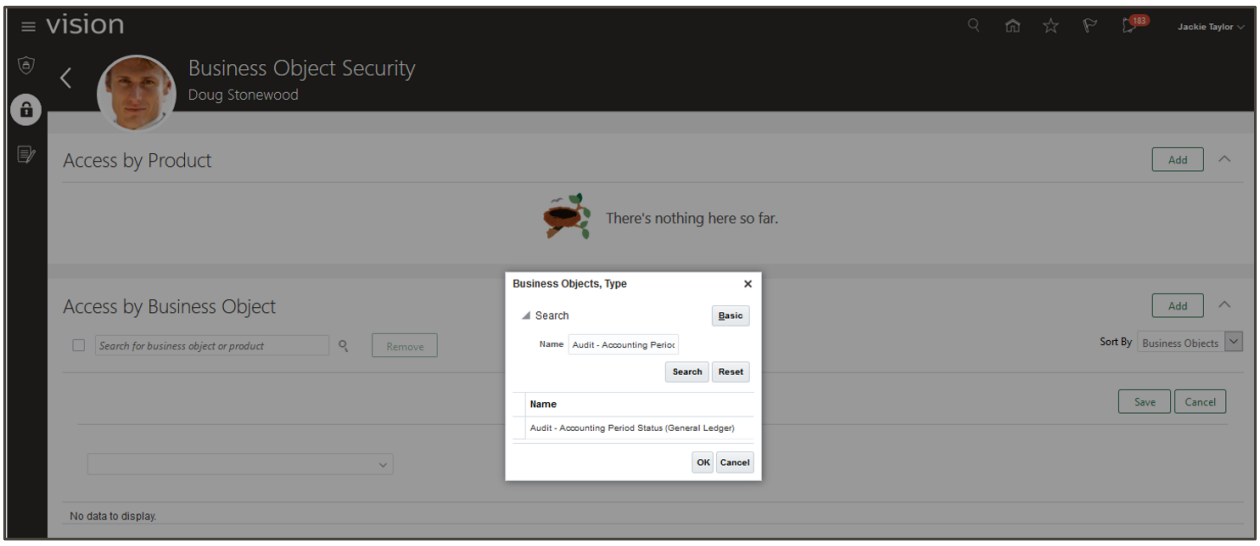


Here, select the Add button for 'Access by Business Object' region instead.

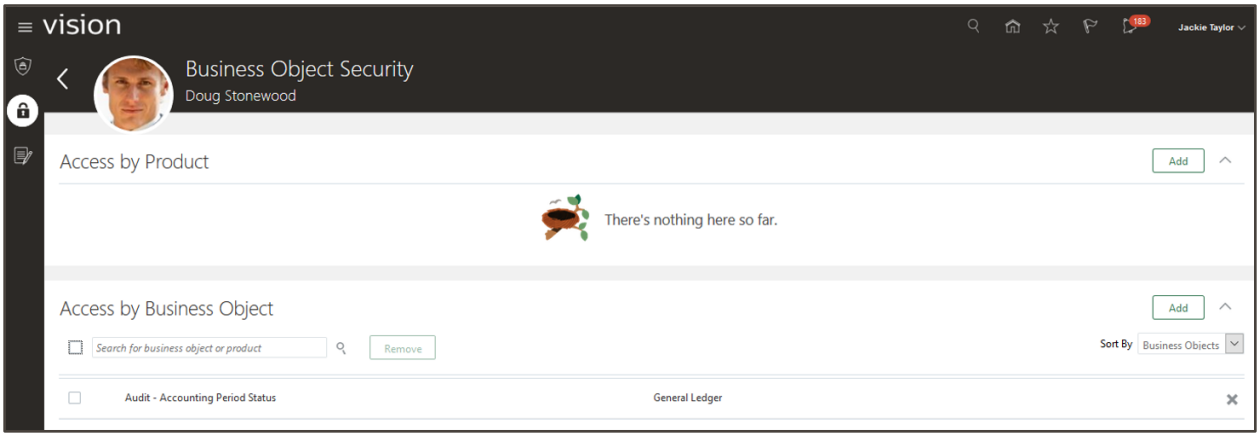


When you know which business object(s) you need to assign, search for them by name. In this example, we want to grant a user business object access to manage or monitor changes to accounting period. Search on 'Audit – Accounting Period Status' to align to these general ledger changes, and Save the business object selected.

Note the delivered best practice model "60018: Updates to Accounting Period Status" uses this business object.

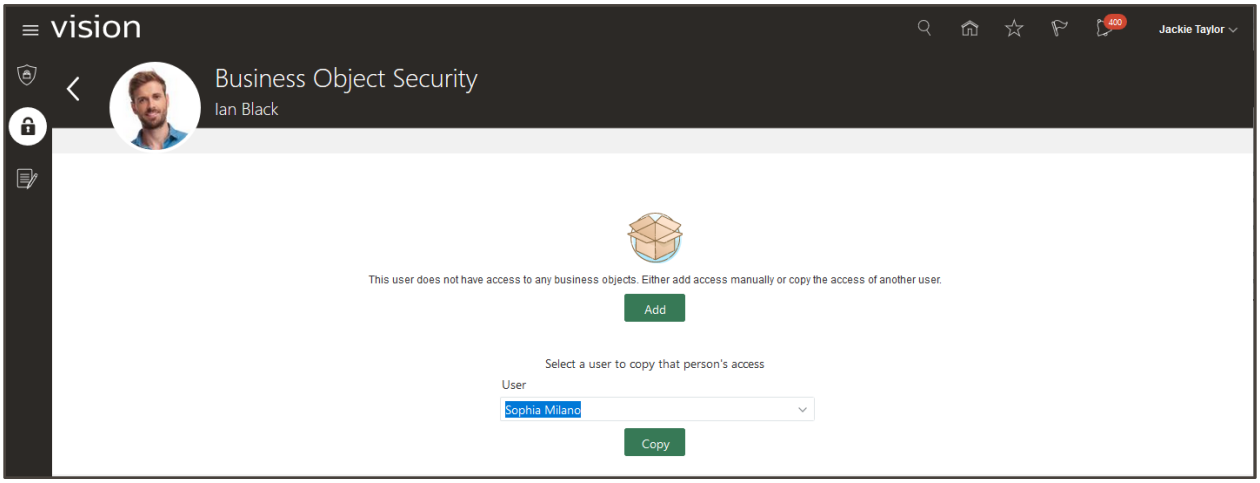


You can continue to add additional business object to the user where required.

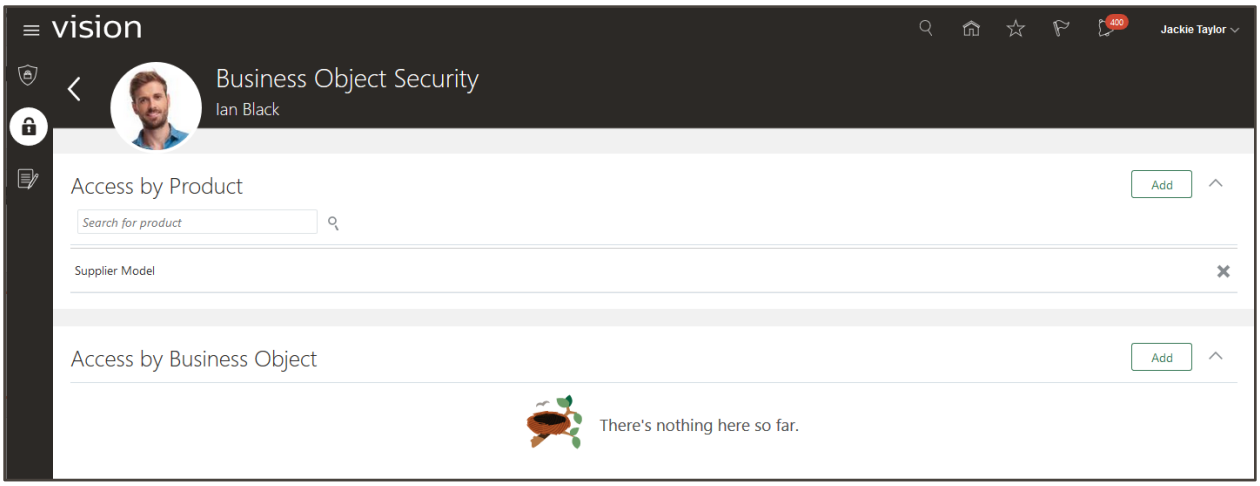


Finally, this example shows you how to leverage a user's existing data security to apply to another user with the same access requirements.

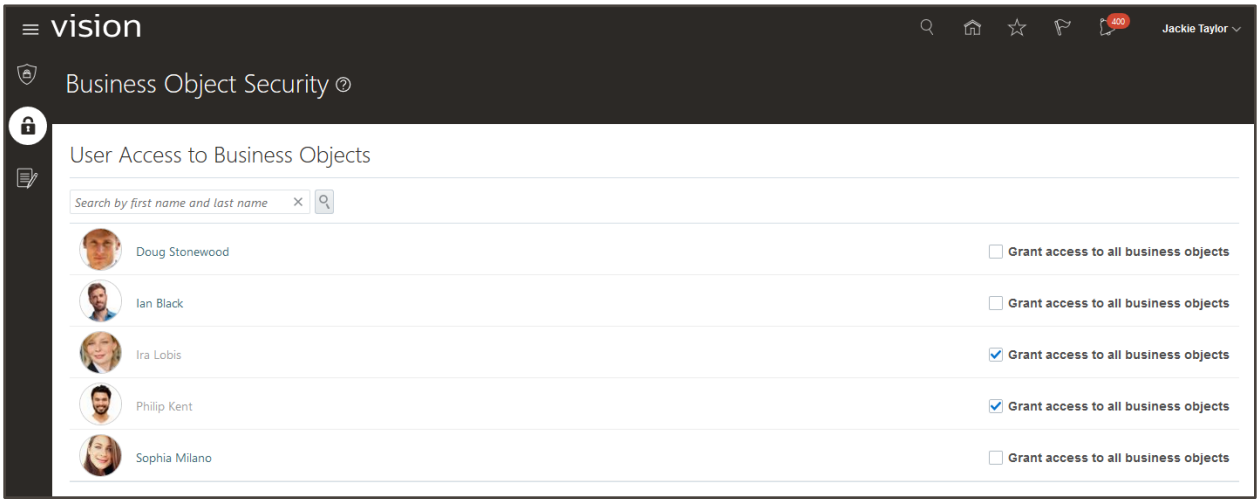
After you select the user's name on the Business Object Security page, in the second half of page there is a drop-down to select a User name to copy their access. Once you select the user name, select the 'Copy' button.



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.



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.

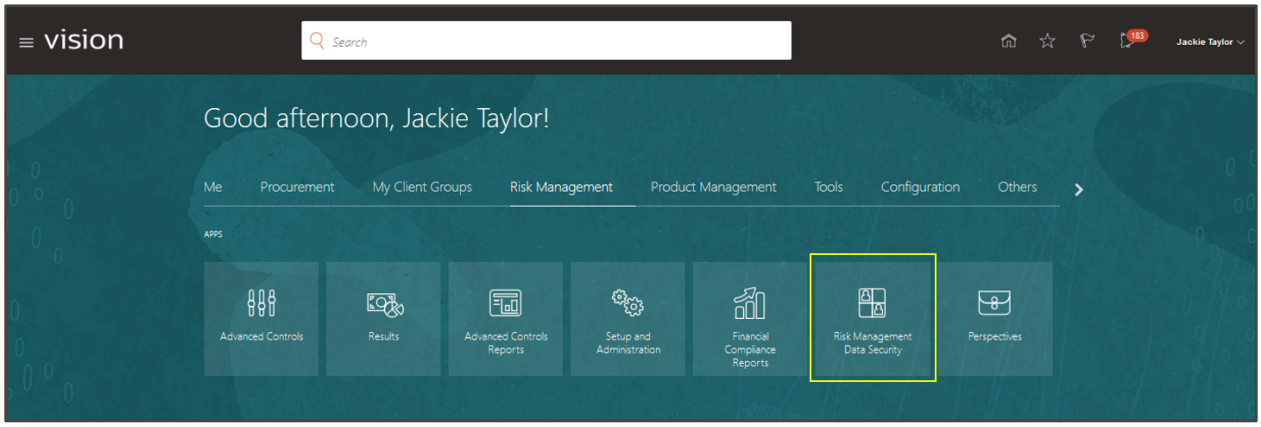
As an overview of this feature, a user group represents one type of data authorization. The criteria includes the data records you can access (objects), and how you can work with the data (authorization). For purposes of this document, there are three object areas we will use here: Transaction Model,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

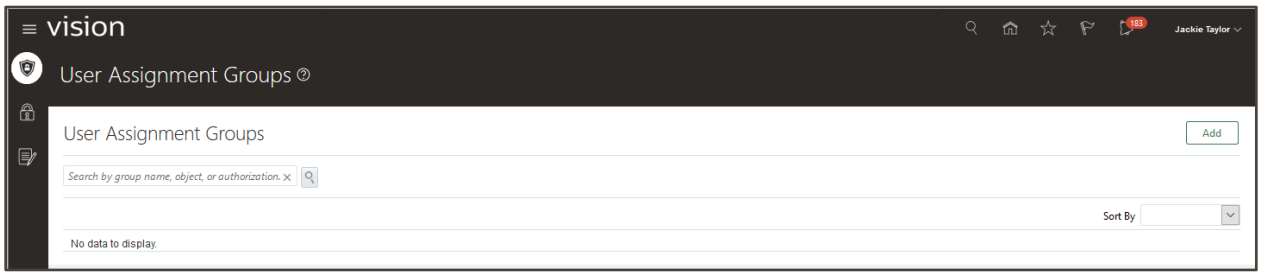
User assignment groups are created and maintained by the risk and compliance administrator. The below will walk through defining user groups for owners in the procure-to-pay business area for configuration controls.

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

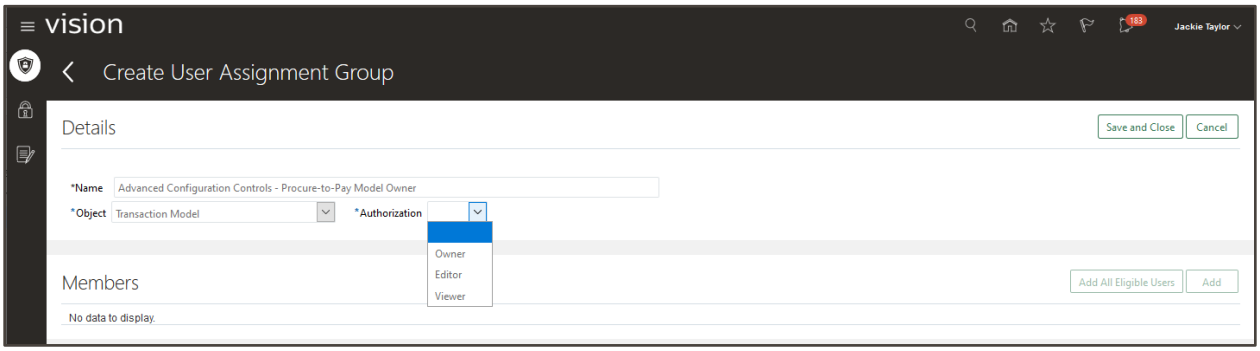


User Assignment Groups for Models

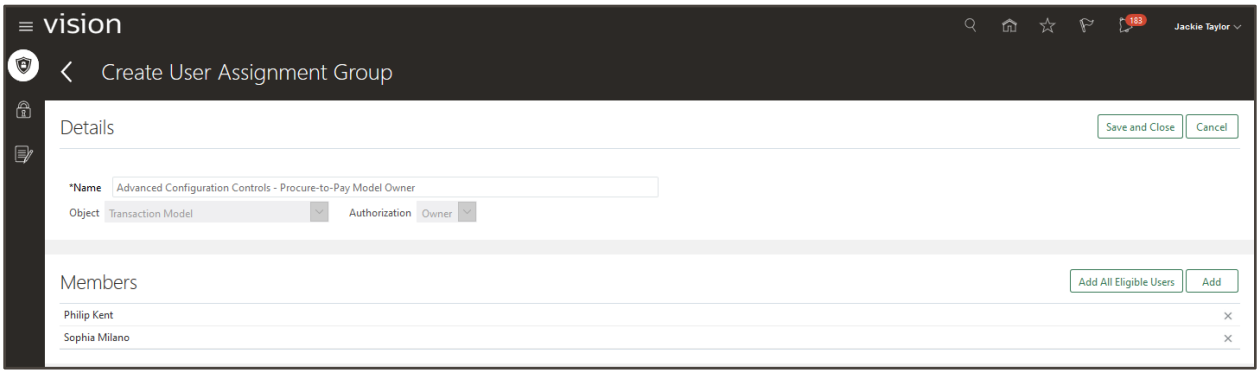
On the User Assignment Groups tab, select the Add button to create a new user assignment group for transaction model owners.



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 Configuration Controls – Procure-to-Pay Model Owner” and will group members who can create, edit, and assign security for configuration 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 Configuration Controls – Procure-to-Pay Control Owner” and will group members who can create, edit, and assign security for configuration 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.

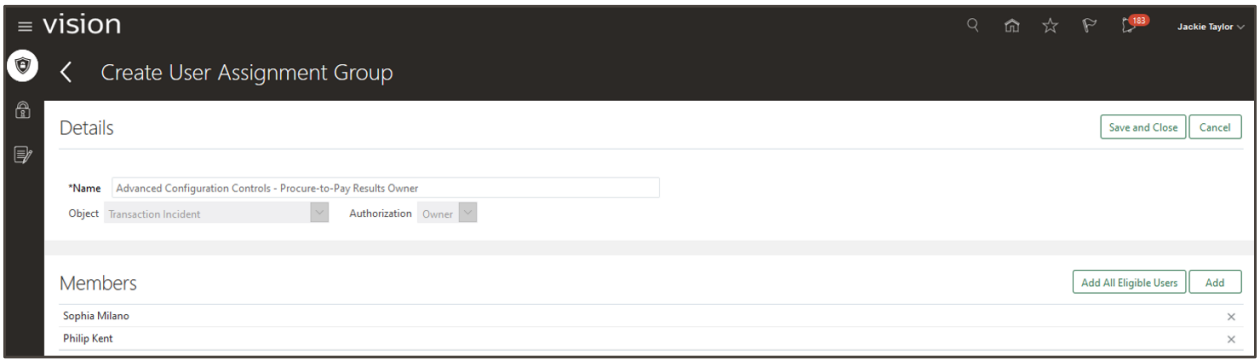
When you have finished defining the group for control owners of the procure-to-pay business area, Save and Close the page.

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 Configuration Controls – Procure-to-Pay Results Owner" and will group members who can edit and assign security for configuration 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.

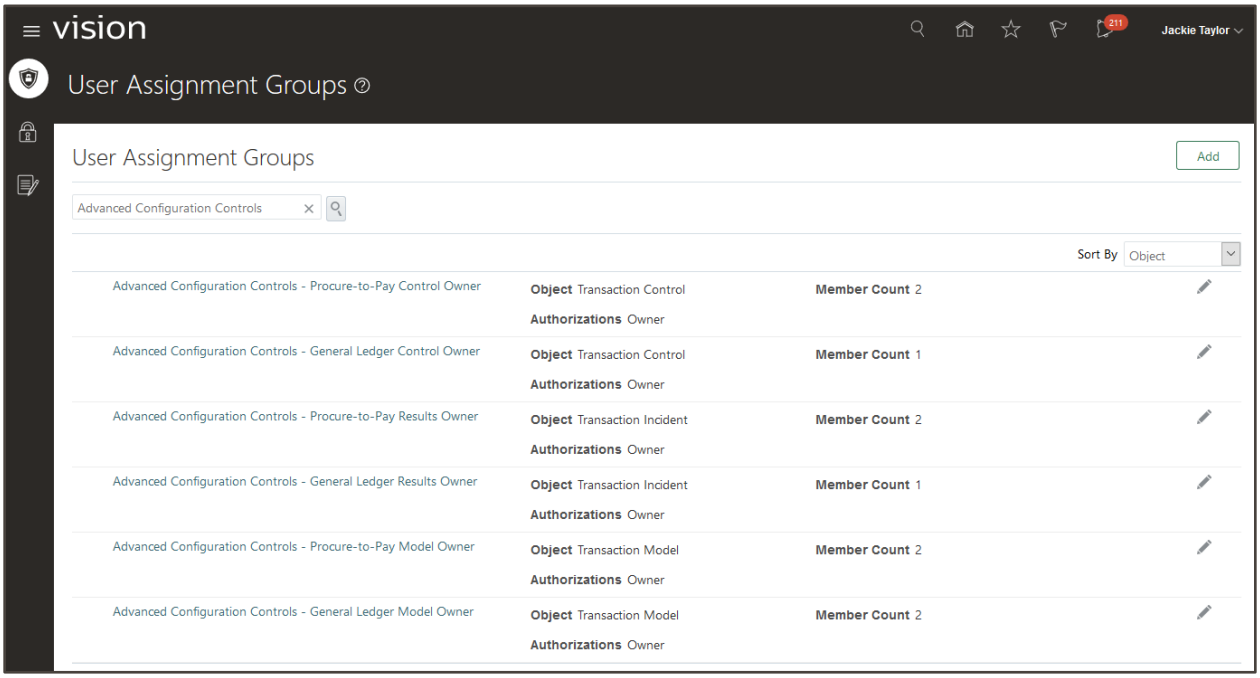
Other User Assignment Groups

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.



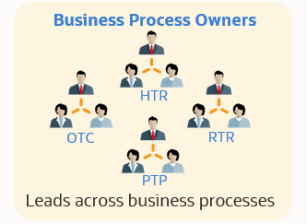
Audit Policy Prerequisite Steps

Overview and Participants

This section will cover the steps required to enable change tracking by application, and leverage this information in Risk Management controls.

Your security team will enable access to configure Oracle Cloud Audit Policies, audit reports, and advanced control to member(s) of the risk and compliance team.

Your risk and compliance administrator will configure Oracle Cloud Audit Policies and verify by using Audit Reports and configuration 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 data for best practice configuration controls and evaluating results.

Step 1: Audit Policy Overview

As a prerequisite to using track change controls in Advanced Controls, you must first configure the Oracle Cloud audit framework for business objects and attributes under Audit Policies. Then, a user must be granted business object access in Advanced Controls to capture the data events logged in a configuration control.

> *Note: The name of each business object in Advanced Controls begins with the word "Audit". For example "Audit - Supplier Sites." Each of these is a parallel version of a distinct object in the Oracle Cloud audit framework. For example, the Audit - Supplier Sites object for use in models and control is a version of an object called "Supplier Sites", under Supplier Model product, in the Oracle Cloud audit framework.*

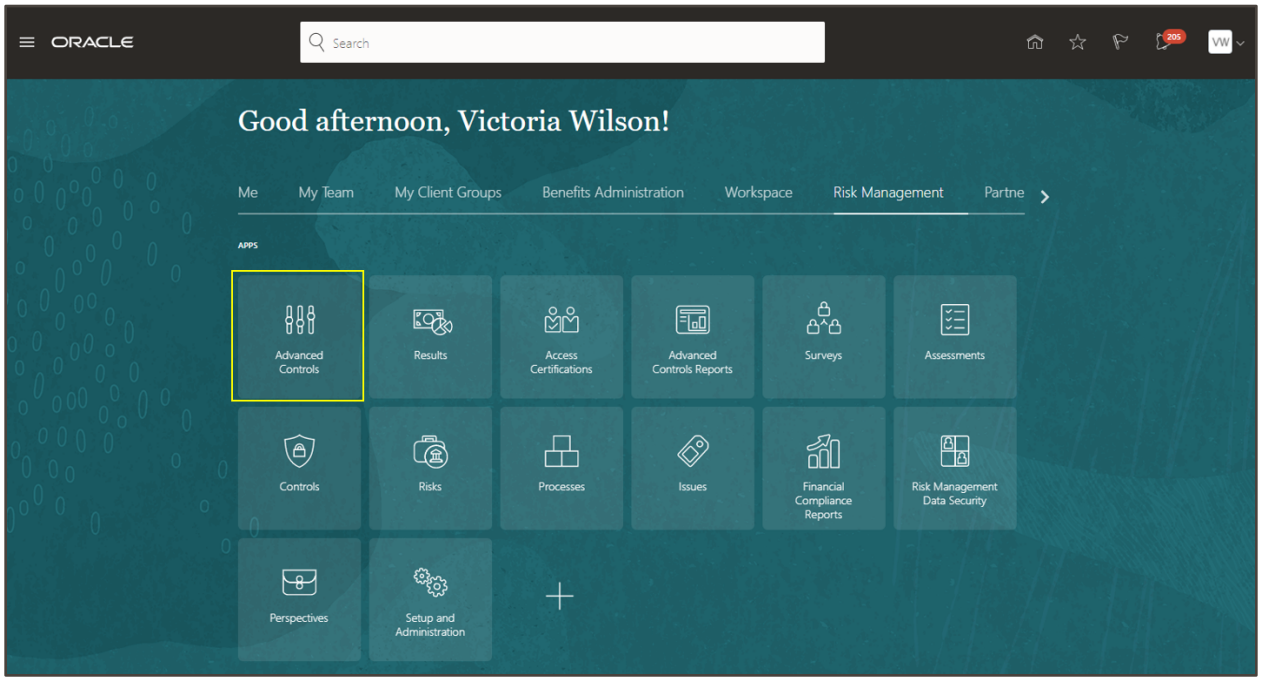
As reference, let's use the delivered best practice ERP model "60001: New Bank Account Added to Supplier" as an example to walk through the configuration process for Audit Policies. You will first need to import delivered content from the Advanced Control library to review the change-tracking attributes, and then configure the corresponding Audit Policies associated to control.

Step 2: Import ERP Audit Models

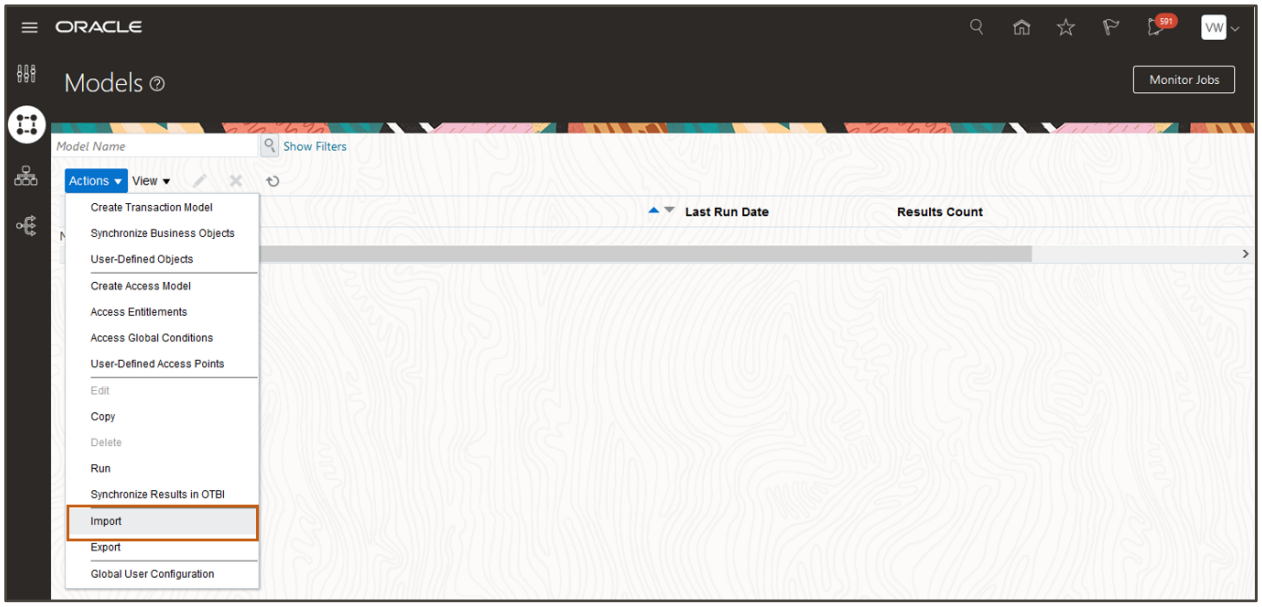
As a user with owner access to transaction models, you can review the attributes tracked by each model that you import from the ERP content library. The attributes in a business object delivered in Advanced Controls corresponds to an Oracle Cloud business object and attribute under Manage Audit Policies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

The security team needs to grant access to the Fusion Manage Audit Policies page to configure change tracking in advanced controls, in addition to setting up business object data security (covered in the prior section).

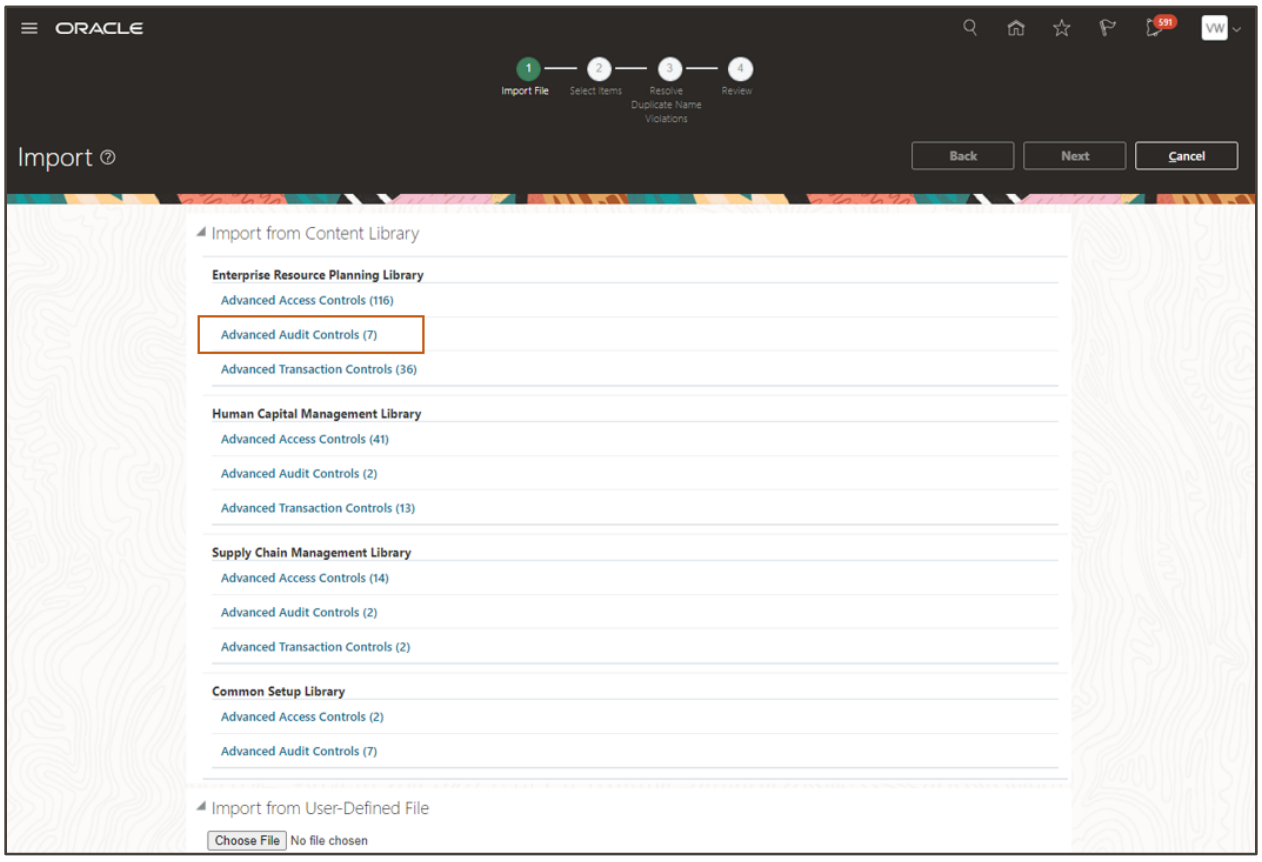
Navigate to Risk Management > Advanced Controls to access the Models page.



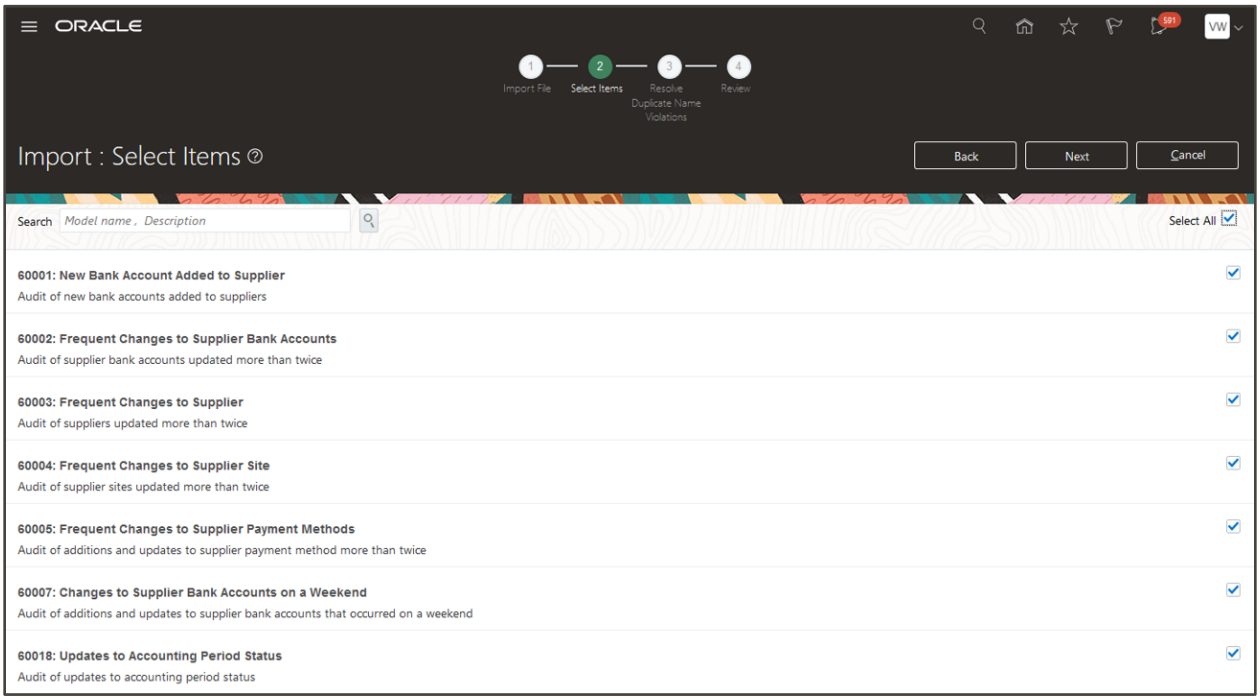
Select the Models tab, and toolbar action to Import from delivered content library.



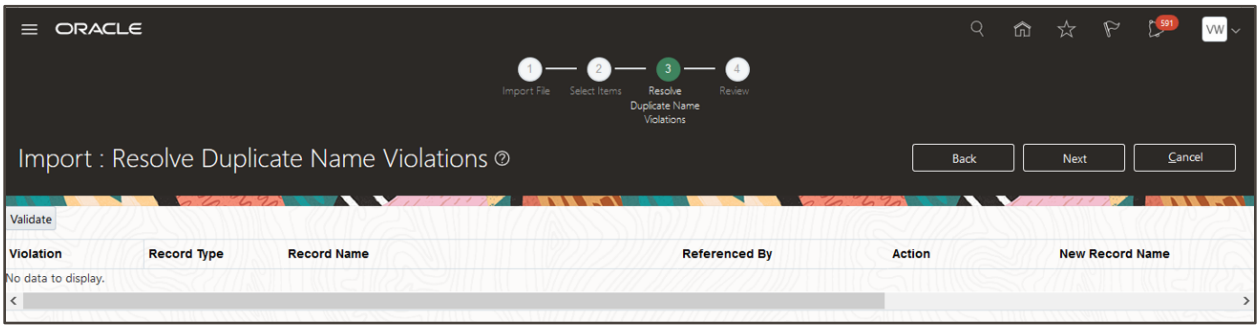
Select the Advanced Audit Controls link under Enterprise Resource Planning Library (ERP). This will return the available delivered content for this business area. There are currently seven available.



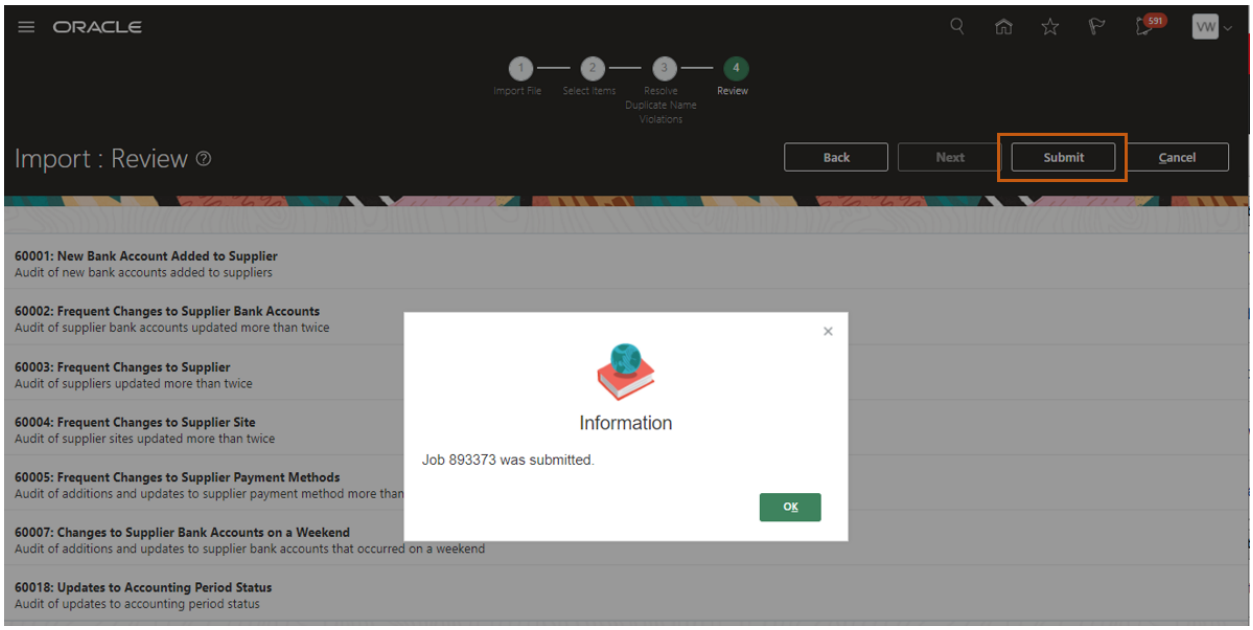
You can ‘Select All’ available ERP models, or pick which models to review and test in this initial configuration control test. Model “60001: New Bank Account Added to Supplier” will continue to be used as an example throughout this document, but go ahead and select them all. Click Next button.



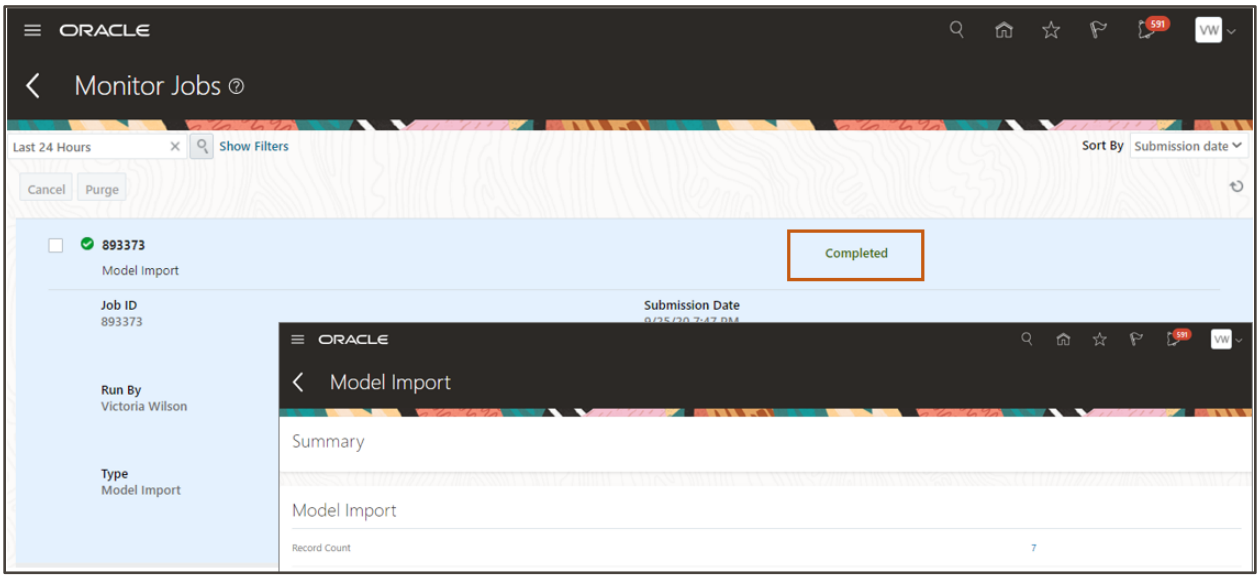
If the delivered model had already been imported before, you will need to Resolve Duplicate Name Violations before moving to next/final page. In this example, this is the first time the models are imported and does not require any action on this page.



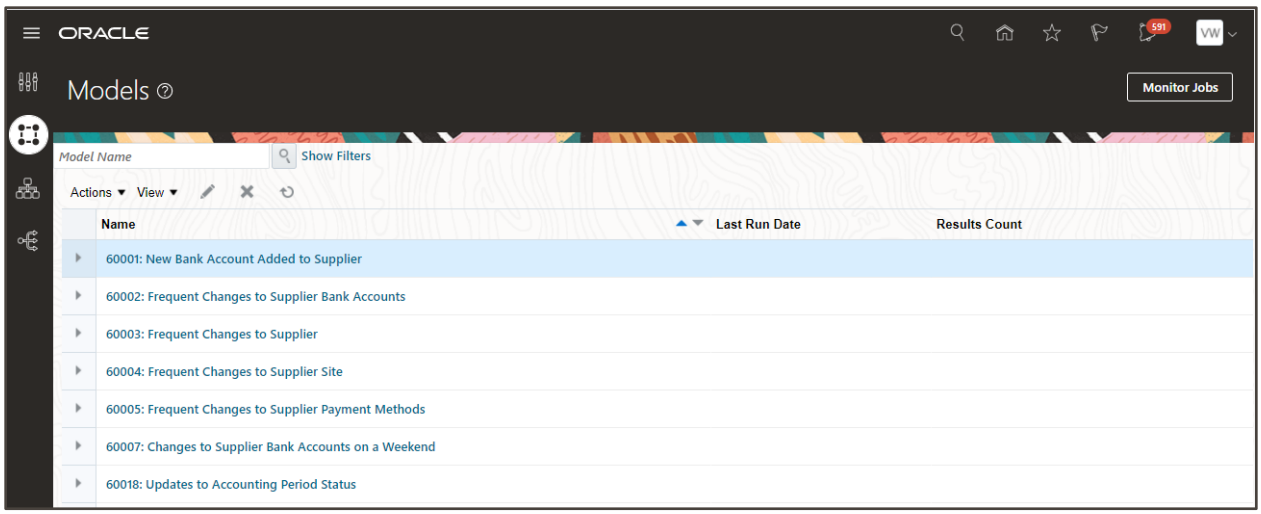
Review the selected models and Submit to import them on this final page. A job is run to import the models and note the job ID.



You can check the job status and confirm that all the selected models 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 all seven models were imported).



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



After you have finished importing your models, another step is required to review them so you know which business objects and attributes will need to be enabled in the Oracle Cloud audit framework.

Step 3: Review the Configuration Model Requirements

For this step, we will continue to use the "60001: New Bank Account Added to Supplier" as an example to walk through requirements. The information identified in this step will be used in following to configure Oracle Cloud audit framework.

While still on the Model page from previous step, select the 60001 model and select Edit pencil icon. In general, a model definition for configuration/transaction type has six key areas, and they include:

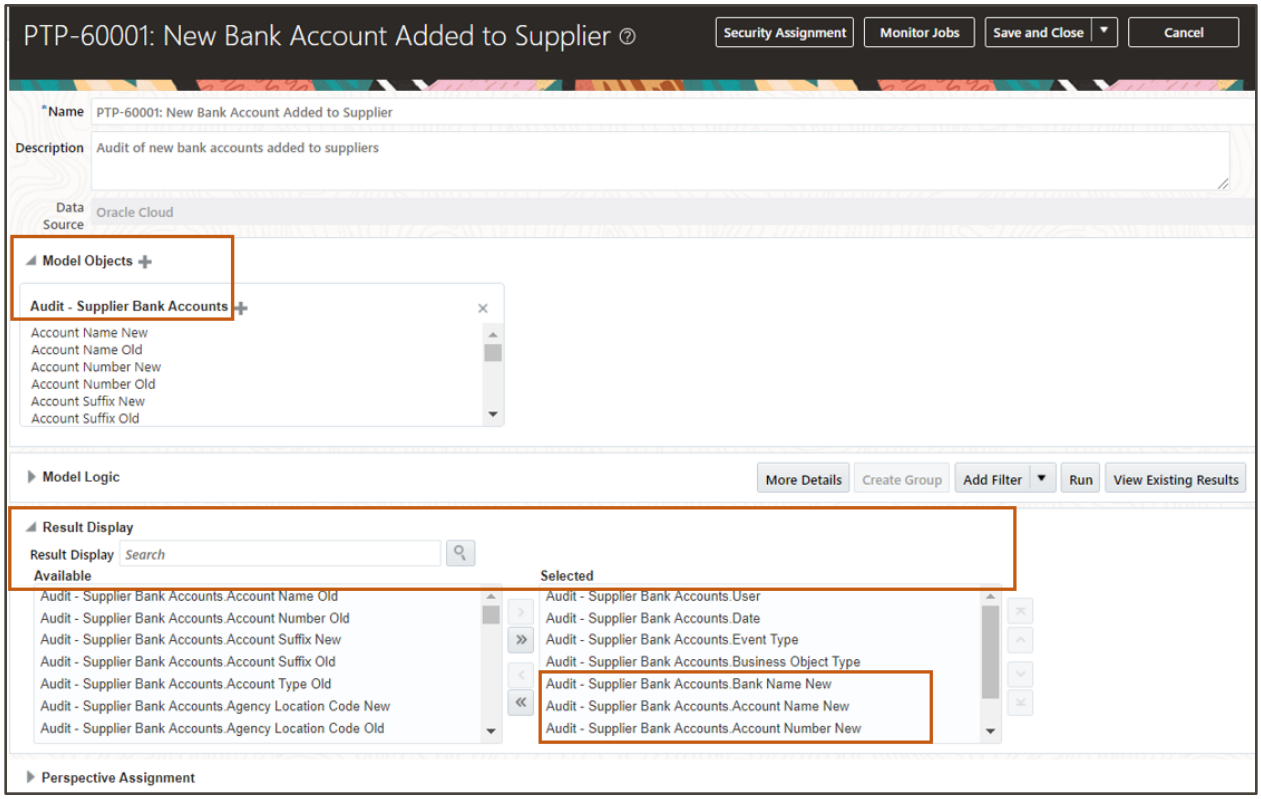
1. Model name and description
2. Security Assignment in the header region
3. Model Objects
4. Model Logic
5. Model Results
6. Perspective Assignment

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.

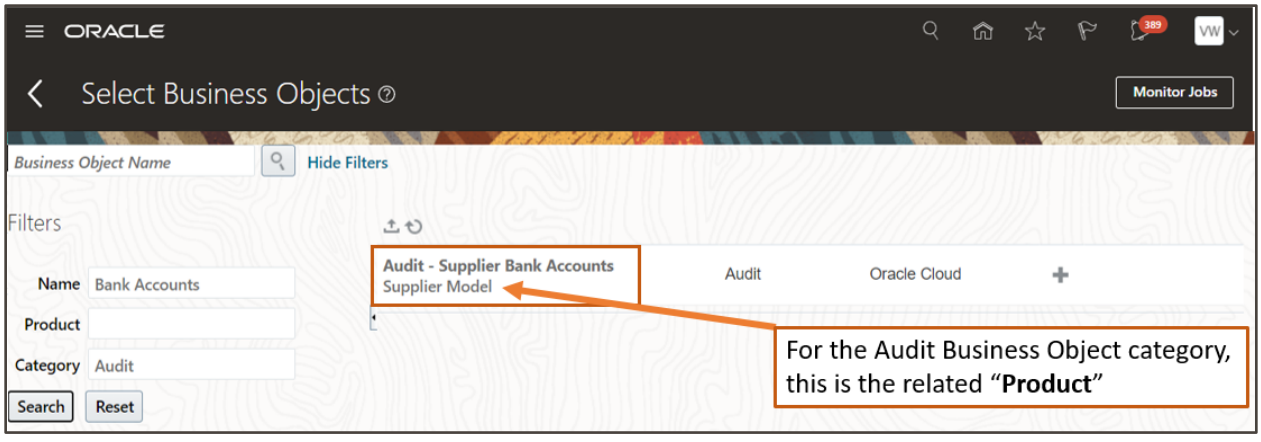
To determine the audit requirements for the configuration model, the focus is on Model Objects (#3) and Model Results (#5) from above list.

As part of reviewing these models, you will rename them to include a business process prefix of "PTP-" or "RTR-". Doing so will help to follow the business process area types, secure users for these areas, and organization in OTBI reporting covered later in this document.

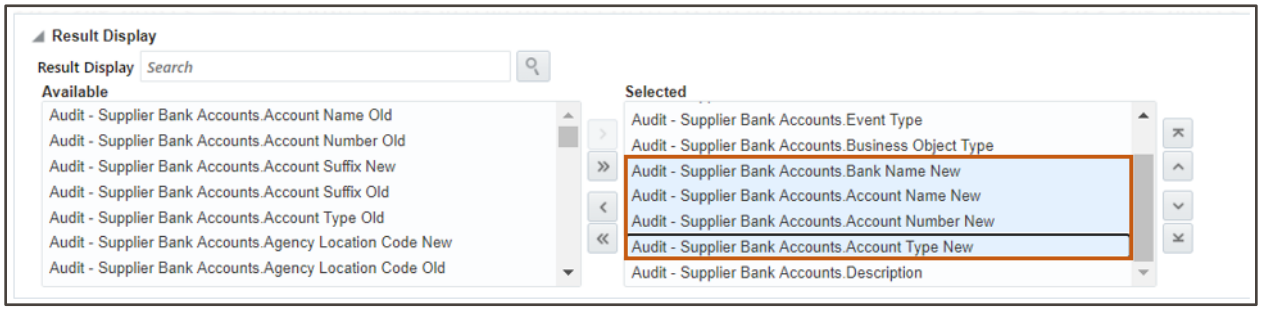
First, click to expand the Model Objects section, and note the business object name is 'Audit – Supplier Bank Accounts' in this delivered model. (The Result Display will be covered after evaluating the business object.)



Second, click the + next to Model Objects to open the Select Business Objects page; it is a library of all available business objects you have access too. Search on the business object used in the delivered model 60001, which is 'Audit – Supplier Bank Accounts'. Alternatively, you can also Show Filters and search by Audit Category value, Name, or Product filters. Note the 'Product' this business object is associated too – <u>Supplier Model</u> - located under the business object name. This indicates the Fusion Application Audit Policy product area that corresponds to event changes such as insert, update, and delete, and will require configuration in that source.



Next, return to the model definition to review the Result Display for 'Selected' attributes. There are contextual attributes included with 'Selected' attributes - such as User, Date, Event Type, Business Object Type, and Description – but of importance are those with suffix of 'New' or 'Old'. Here, for 60001, this model only includes 'New' attributes because it is for new bank accounts (insert events). The audit attributes required for this model include the following highlighted attributes selected in the screenshot of model definition:



Based on the definition for this delivered audit model, we can determine the following attributes for 'Supplier Model' Product used for this requirement:

- Bank Name
- Account Name
- Account Number
- Account Type

Perform the same steps for the other imported ERP audit models. Also, revise the model names to use a prefix of "PTP-". As mentioned earlier, this prefix information will be leveraged in OTBI reporting to group controls together by business process area. Note:

- All models using business objects for 'Supplier Model' Product with have this "PTP-" suffix.
- For the model 60018, it uses a business object for general ledger and should be prefixed with "RTR-".

This step is required because the business object and attributes to be audited in the Oracle Cloud audit framework correspond to delivered business objects used in advanced control models, and depend on these updates to return potential incidents. Enabled Audit Policies stores information related to creation, modification, and removal of business object attributes without any intervention from user when configured for Fusion Applications.

Finally, the table below provides a list of business objects and attributes used in the delivered ERP audit models that will assist you in performing the next step to configure the Audit Policies.

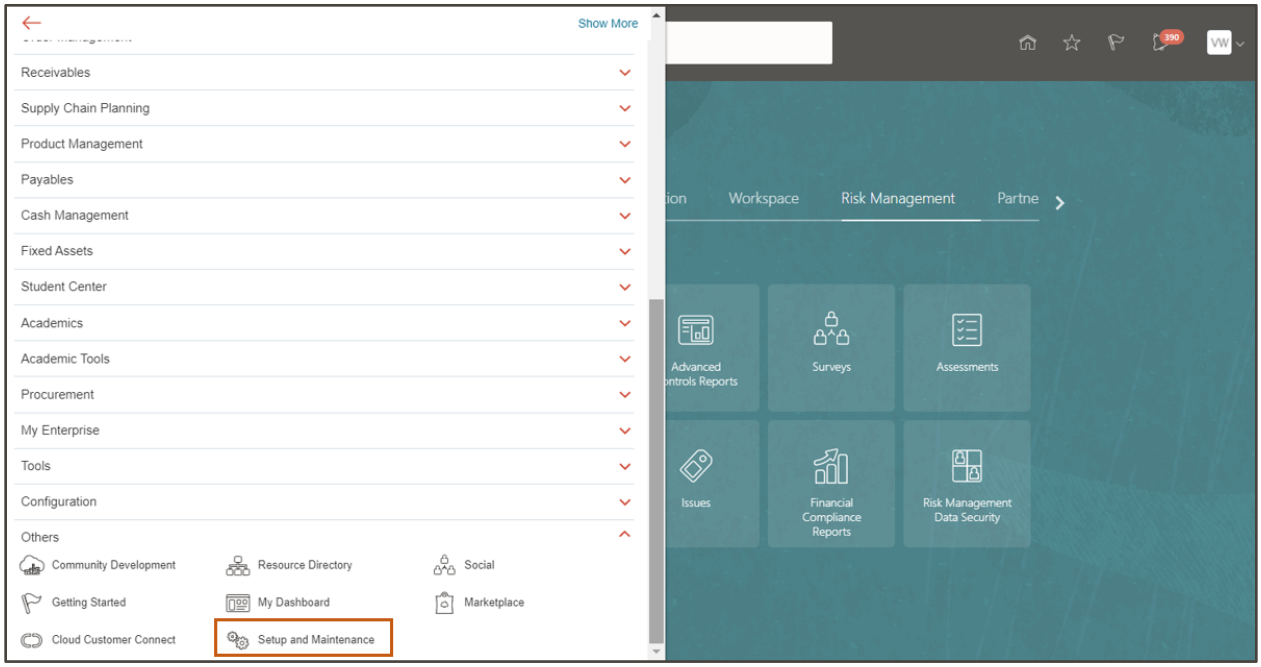
Product (Audit Policy)	Business Object	Attributes
Supplier Model	Supplier Bank Accounts	Account Name Account Number Account Type Allow International Payments Bank Name
	Supplier	Inactive Date One-time Supplier Supplier Type Tax Organization Type
	Supplier Sites	Address Name Inactive Date Payment Terms Site Status
	Supplier Payment Methods	Default Payment Method
General Ledger	Accounting Period Status	Accounting Period End Date Ledger Period Number Period Type Start Date Status Year

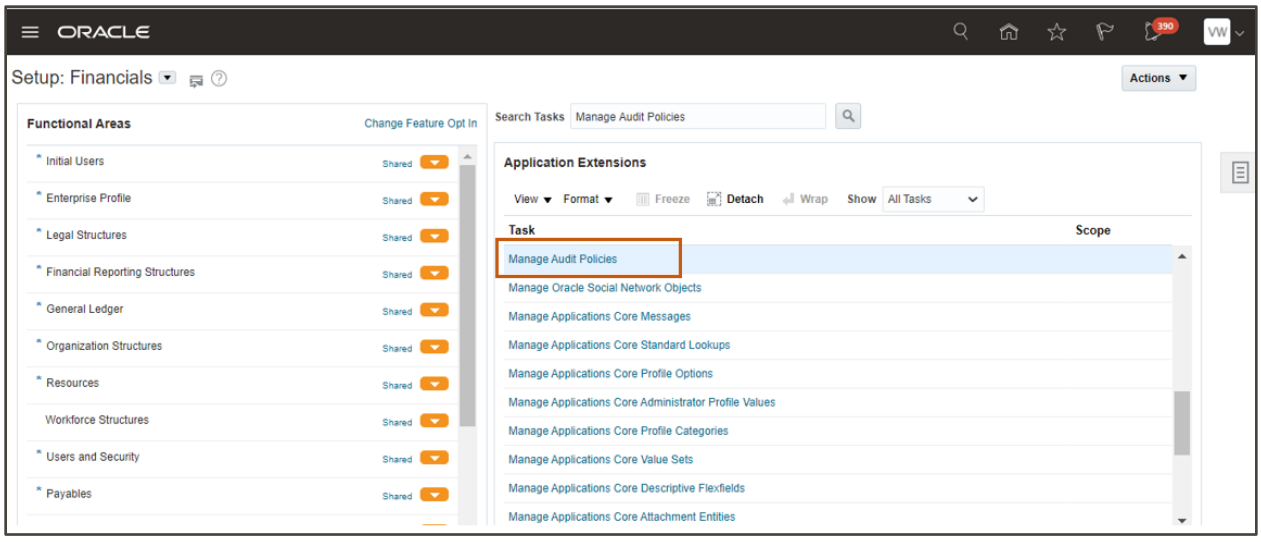
Note: You should only enable attributes you plan to track; performance can be negatively impacted when you enable business objects and attributes you do not need.

Step 4: Configure Audit Policies

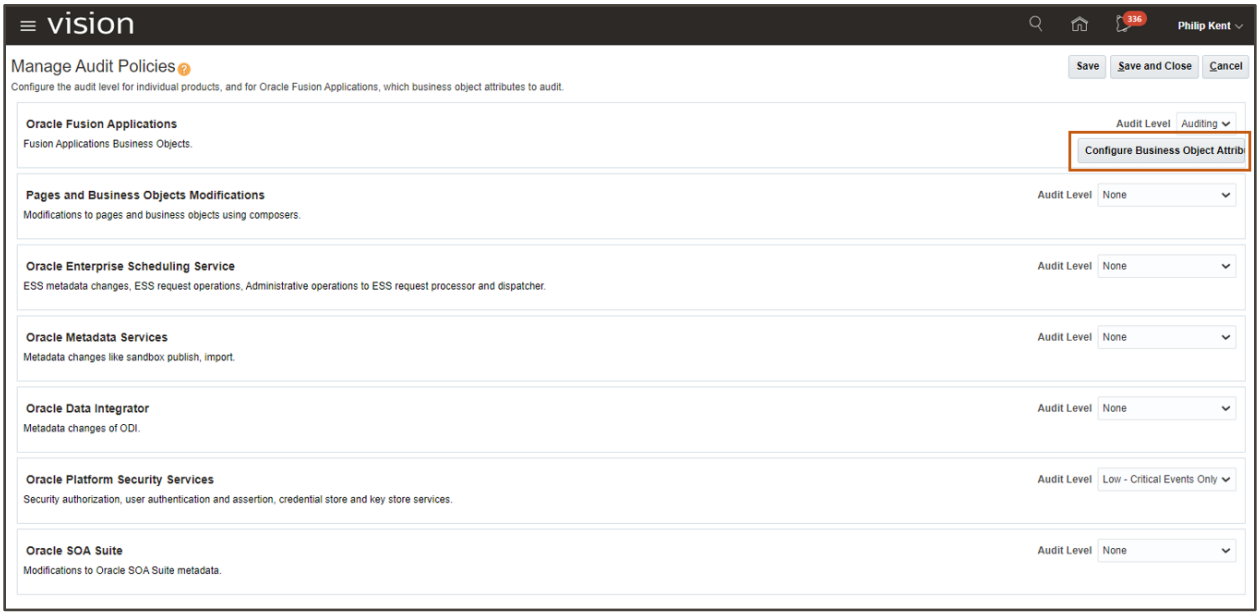
For configuration models that depend upon the Oracle Cloud audit framework, you must first configure this audit-level information. Models and controls that use audit business objects in Advanced Financial Controls can only return data after the corresponding setup is enabled, and after additions or changes have actually been made to the object and attributes.

Navigate to Setup and Administration, and search for the Manage Audit Policies task.

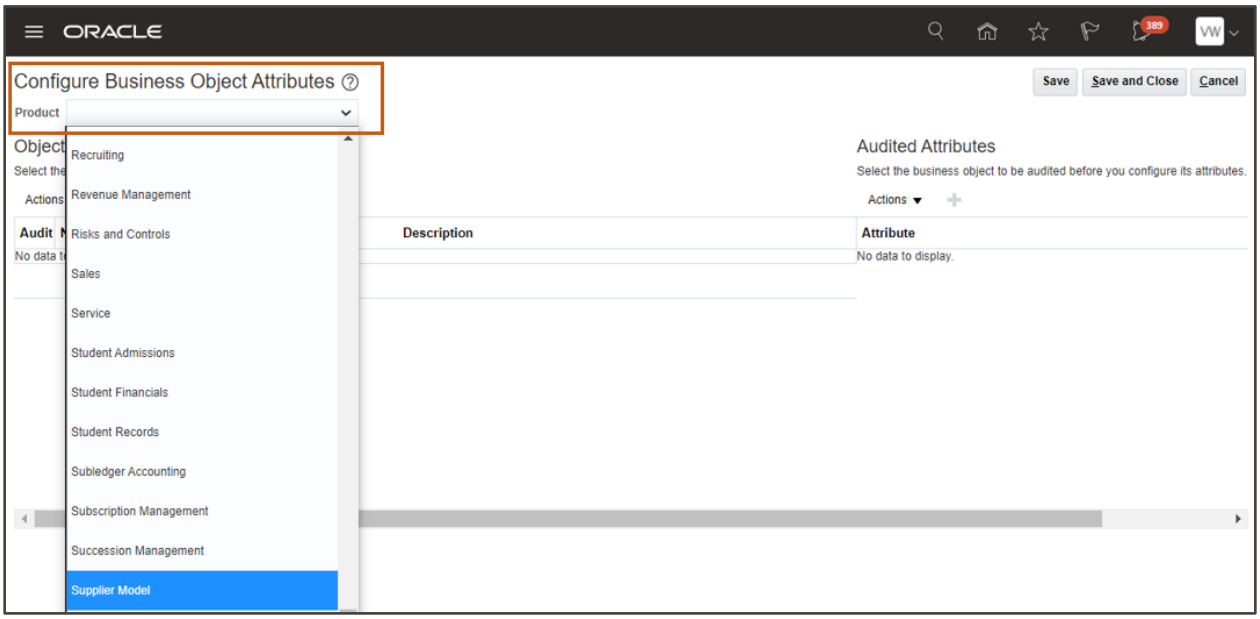




On this Manage Audit Policies page, select the 'Configure Business Object Attributes' button across from Oracle Fusion Application. Business objects and the related attribute data in Advanced Financial Controls come from this policy area of auditing.

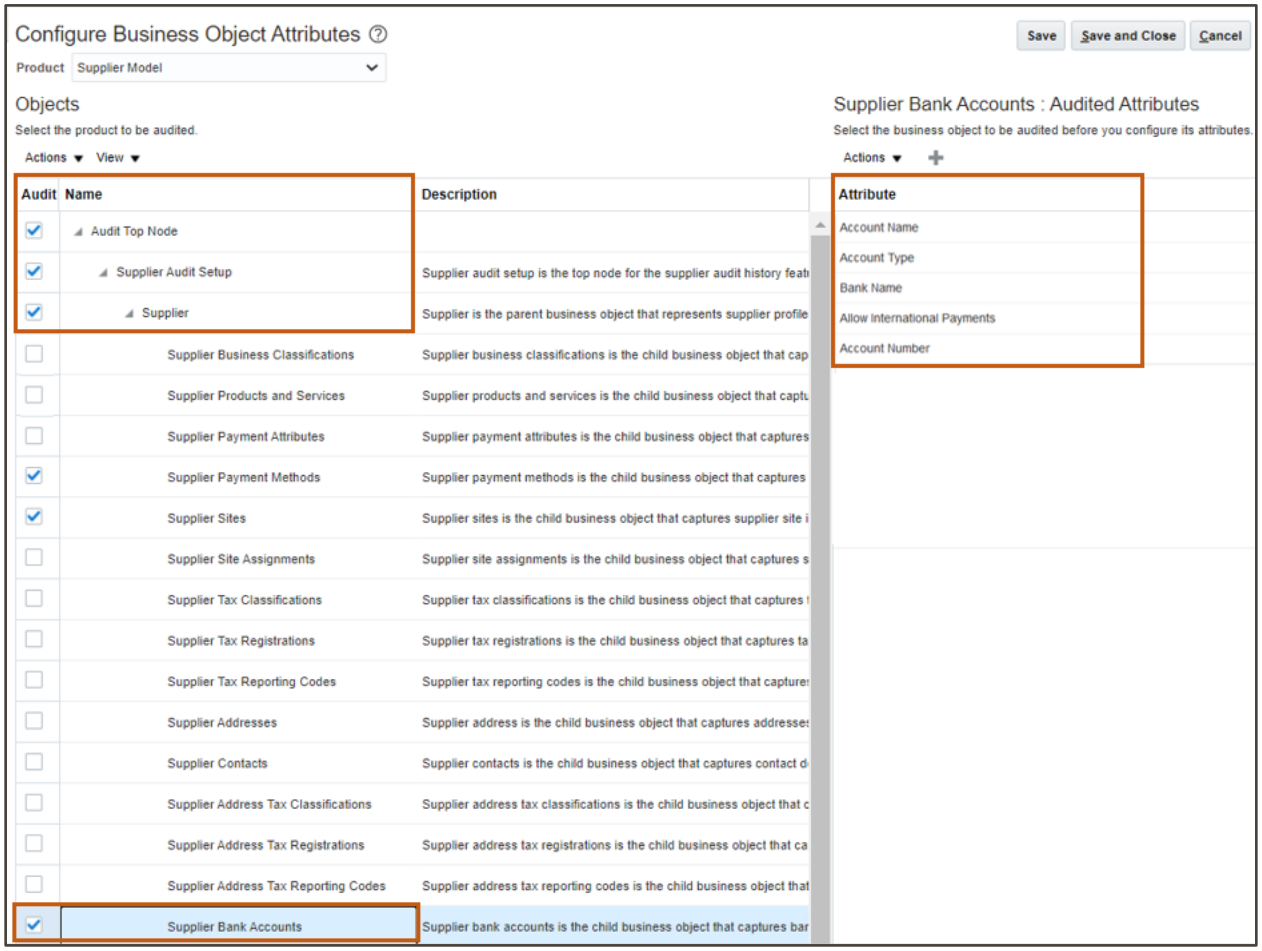


Based on the previous information, you know that supplier bank accounts falls under the Product Supplier Model. At the top of the Configure Business Objects Attributes page, select the 'Supplier Model' Product value from the drop-down.

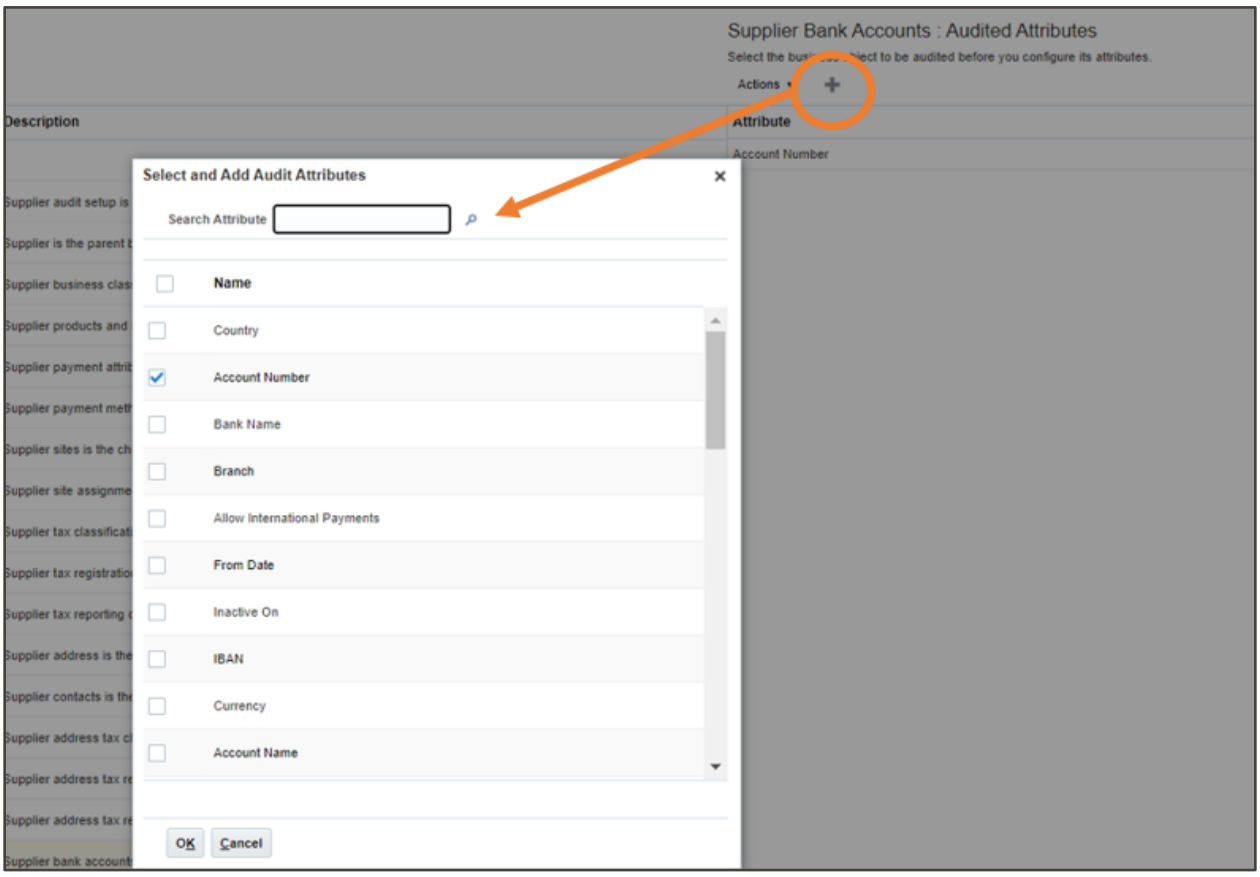


For each business object you use in Advanced Financial Controls, select the checkbox on the left. In addition, you must also select any parent node above the business object to enable the auditing.

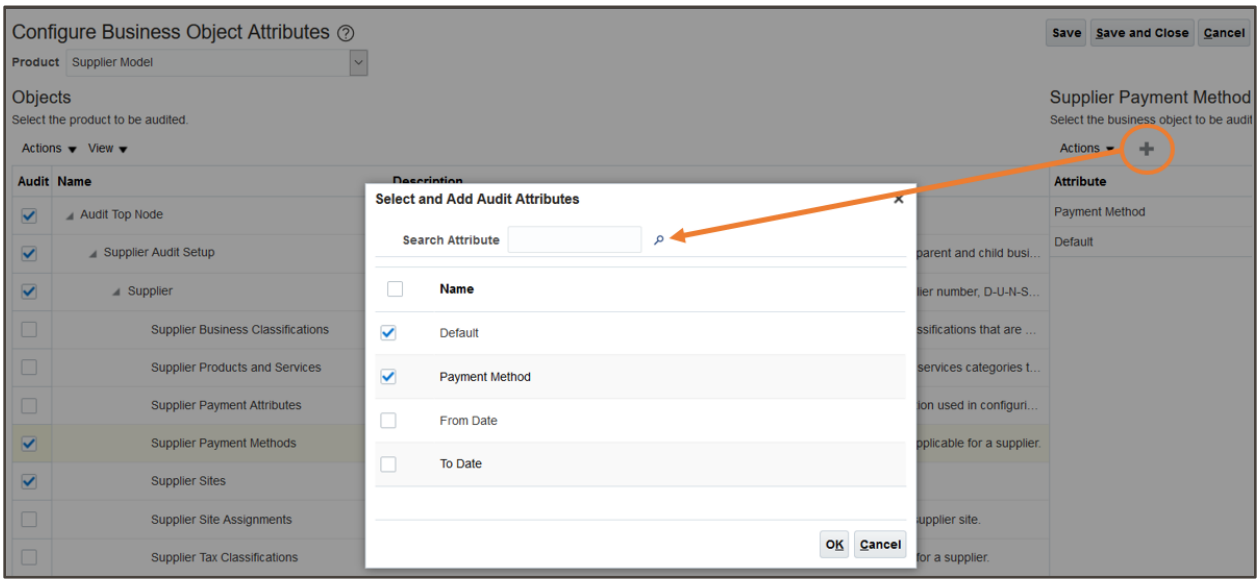
Here in this example, Supplier Bank Accounts is selected/enabled, along with the parent nodes above this business object. On the right-hand side of page is listed the attributes selected to change track.



To add the attributes to change track, you select the + in that right-hand column, or Action > Create, and a popup becomes available to search and add the attributes to track. The below is an example of the business object for Supplier Bank Accounts.



This example is for the attributes selected for the business object Supplier Payment Method.



Using the table provided in the previous step, continue selecting the necessary business objects and attributes you will need for the seven ERP audit modes that have been imported.

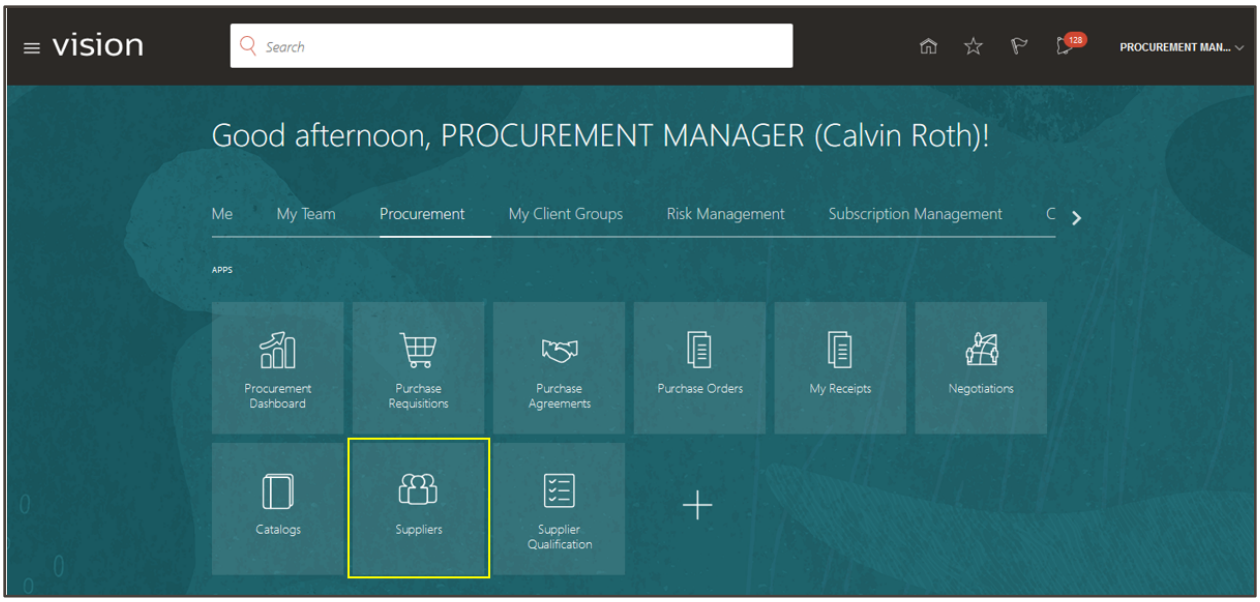
Important: Changes are tracked at the point in time they have been configured.

Step 5: Enter Some Test Data

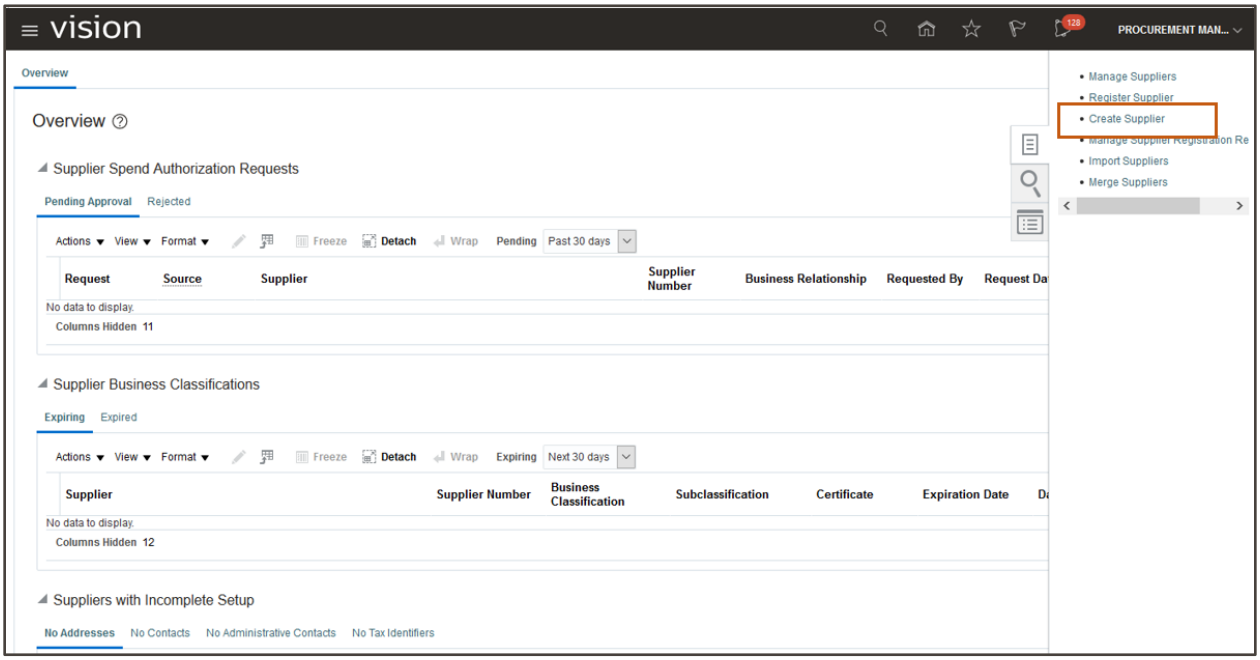
Business process users for ERP configuration controls who would enter test data include those who work with procure-to-pay and general ledger.

In your development environment, add a new bank account for a selected supplier. (You must have the Supplier Manager job to enter new suppliers.)

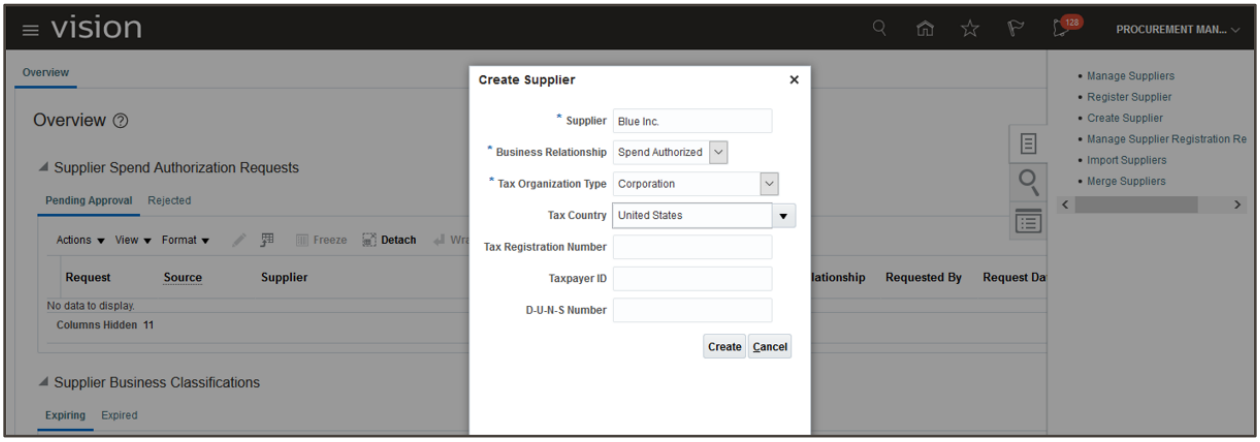
Navigate to Procurement > Suppliers.



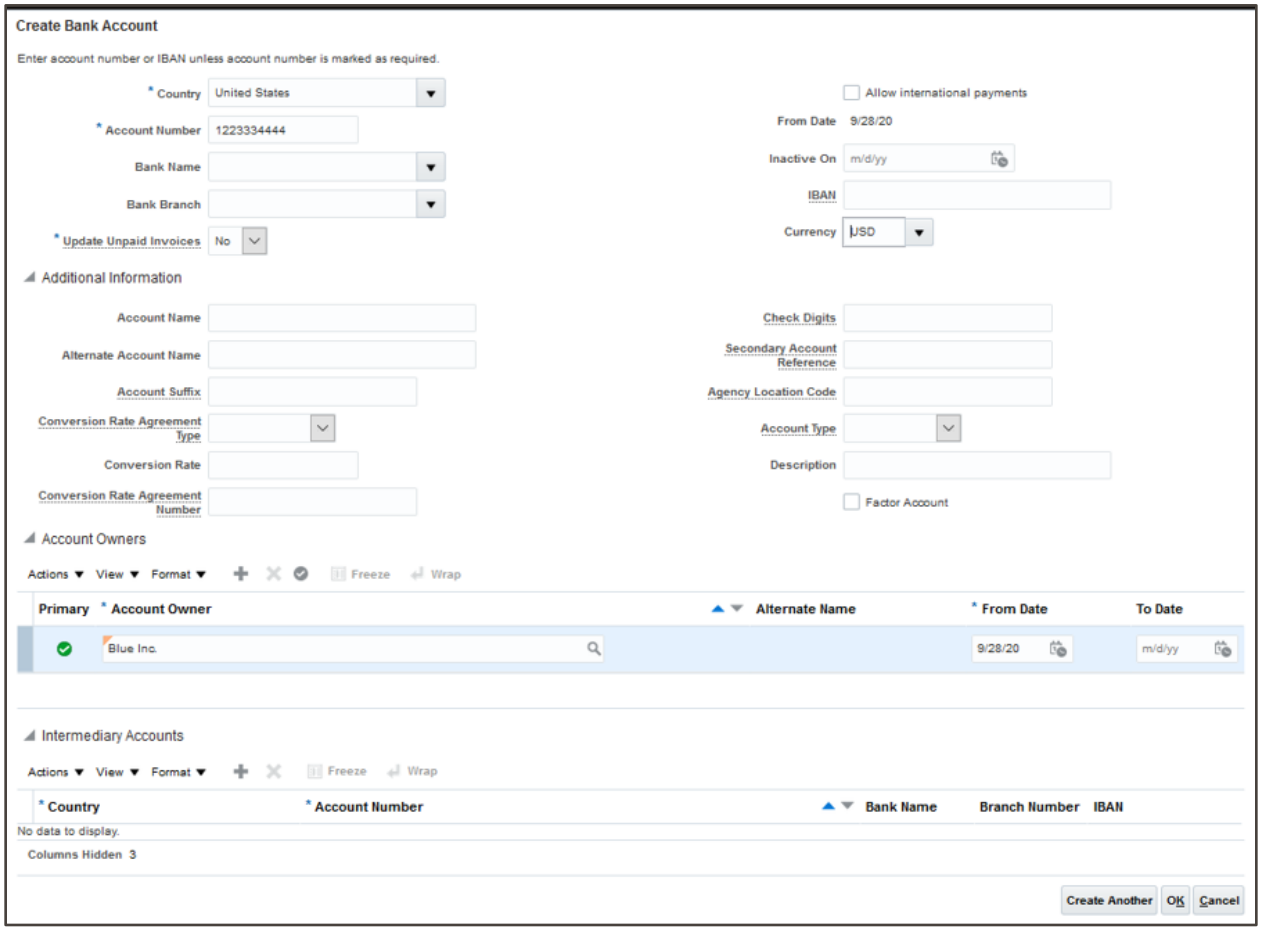
Select ‘Create Supplier’ task.



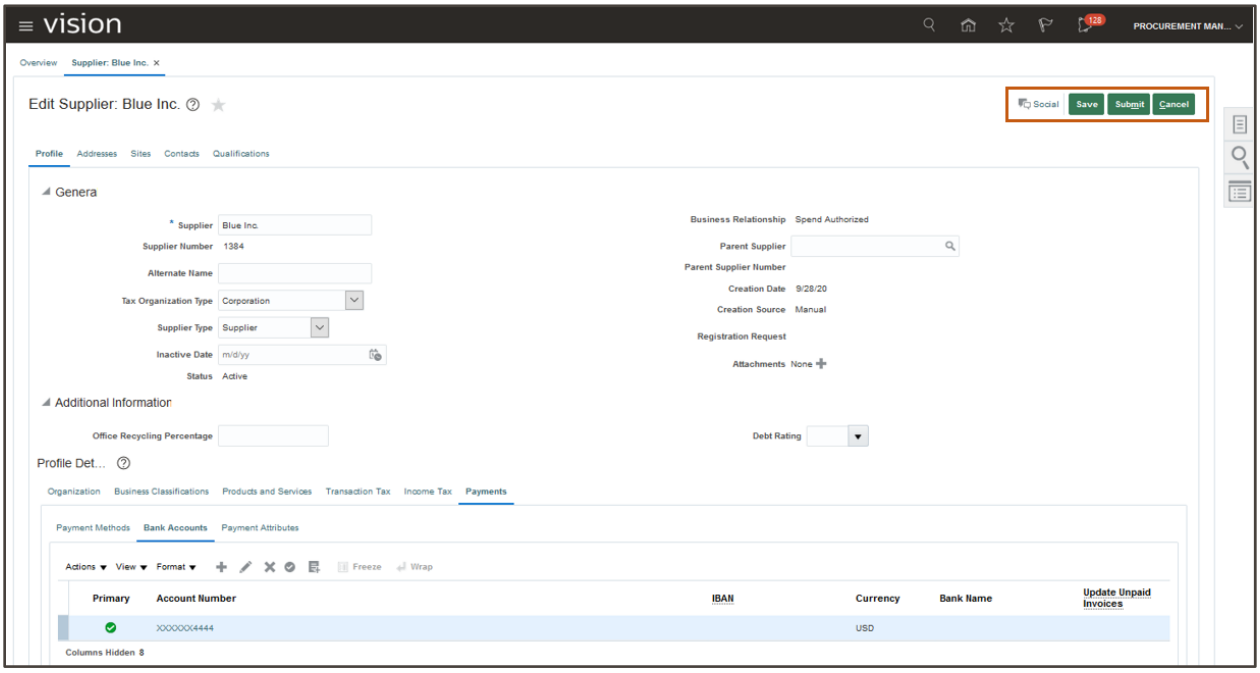
Enter required supplier criteria, such as the name, business relationship, and tax organization type.



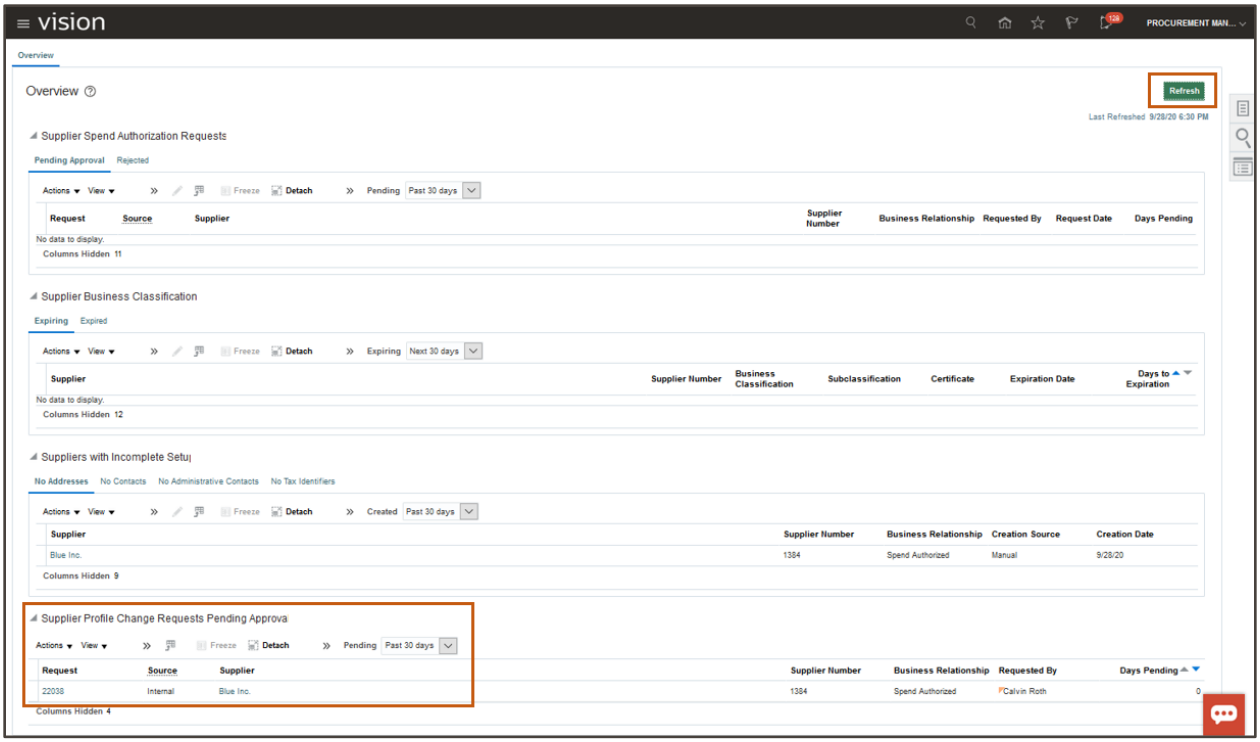
To test configuration settings around newly added bank accounts, be sure to add a bank account to a new or existing supplier. Model 60001 will identify new bank account events (inserts), while model 60002 will identify update events.



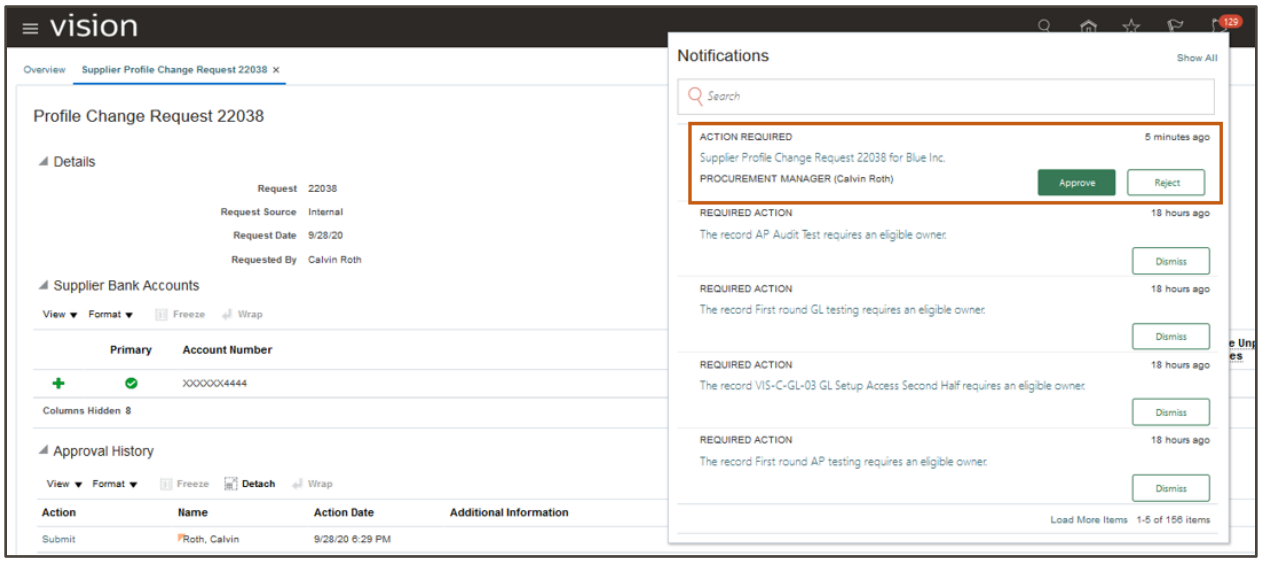
You can Save changes to the supplier record, or when done, click Submit.



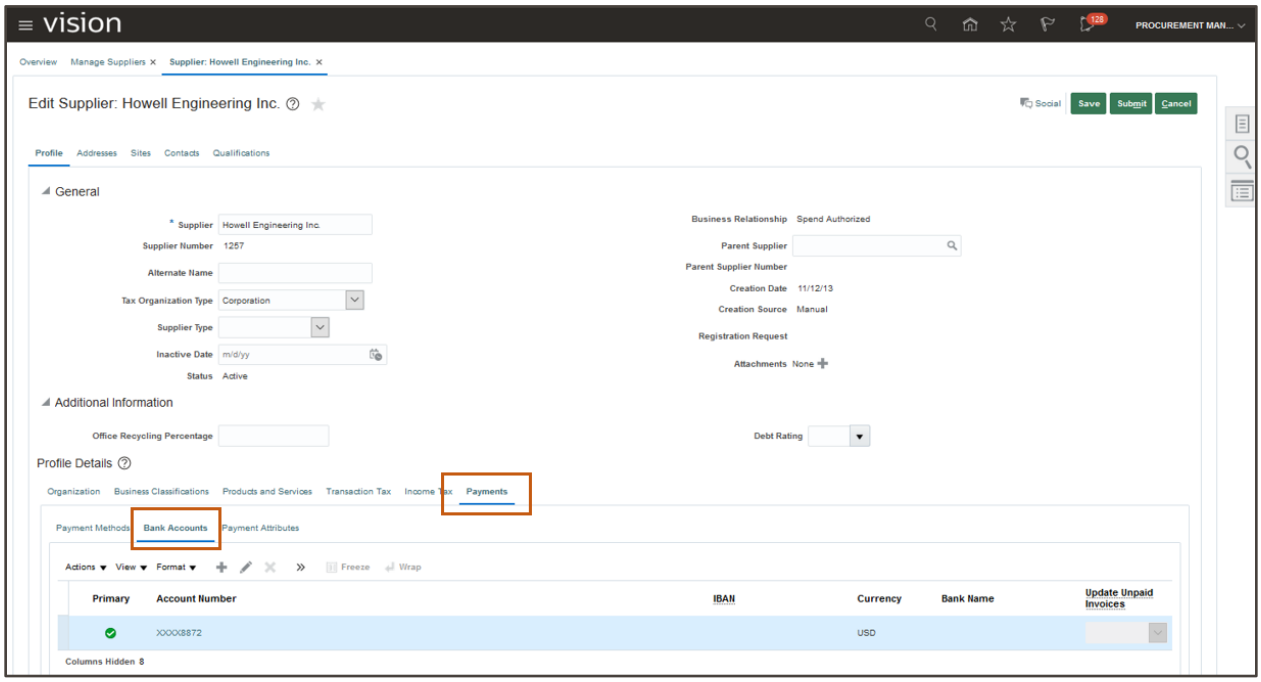
Return to the Overview page to review any outstanding requests; you may need to click 'Refresh' to update any requests. Depending upon how you have your development environment approval and workflow configured, another user may need to approve the new supplier or any bank account changes.



When user action is required, they access the Notification bell in header and perform the approval action.



To make changes to an existing supplier bank account, edit the record and navigate to Payments > Bank Accounts on the supplier Profile. Select the bank account to edit and following the same Submit and approval process, if required. Bank account information can also be added or updated under Addresses or Site level of the supplier.

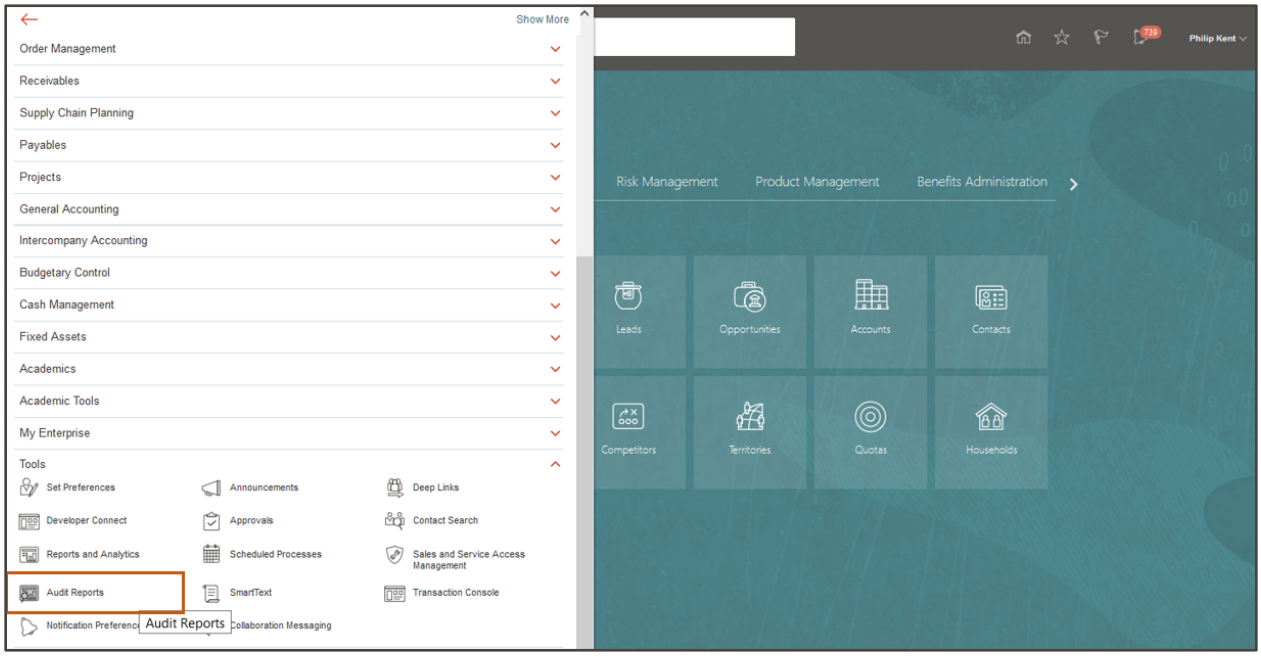


Continue to have your business process owners – such as procure-to-pay and general ledger – make changes in the development environment to provide test data to validate controls and results.

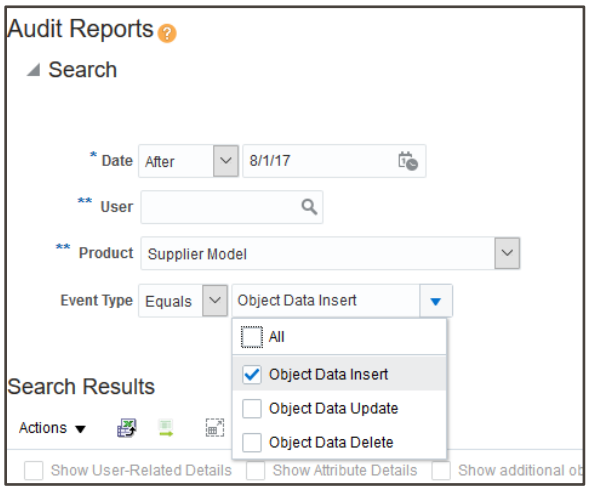
Step 6: Review Changes Under Audit Reports

Once changes are made, you can also confirm these events using the Audit Reports tool to preview the information.

To access Audit Reports, navigate to Tools > Audit Reports.

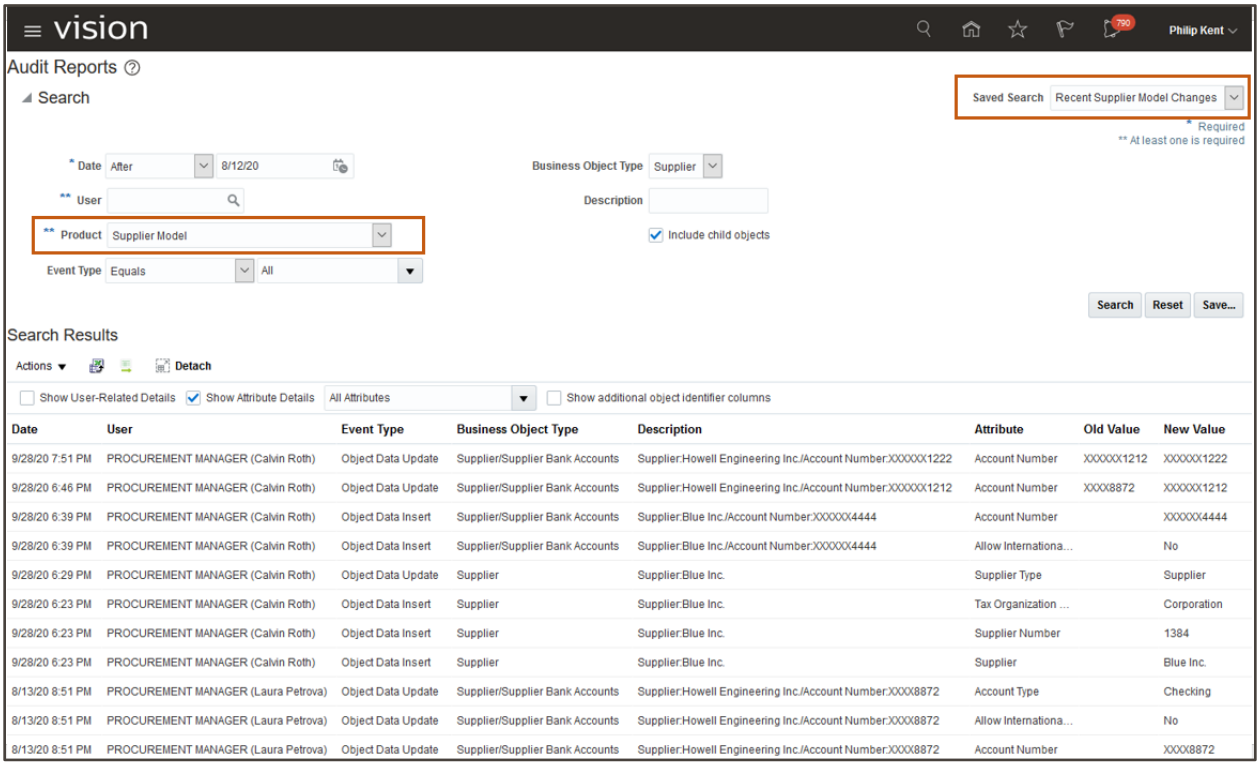


In the top Search region of page, you enter criteria around date of events, the Product (Supplier Model), and event types and click Search. For the event types, you can select All, or those for specific actions of inserts, update, or delete.

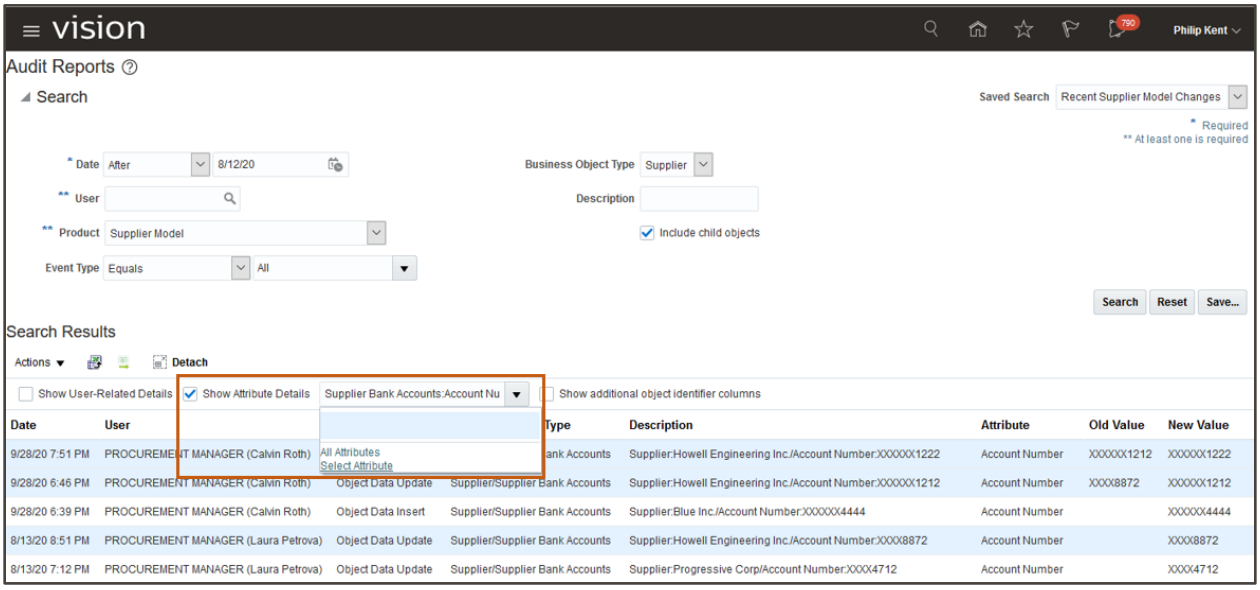


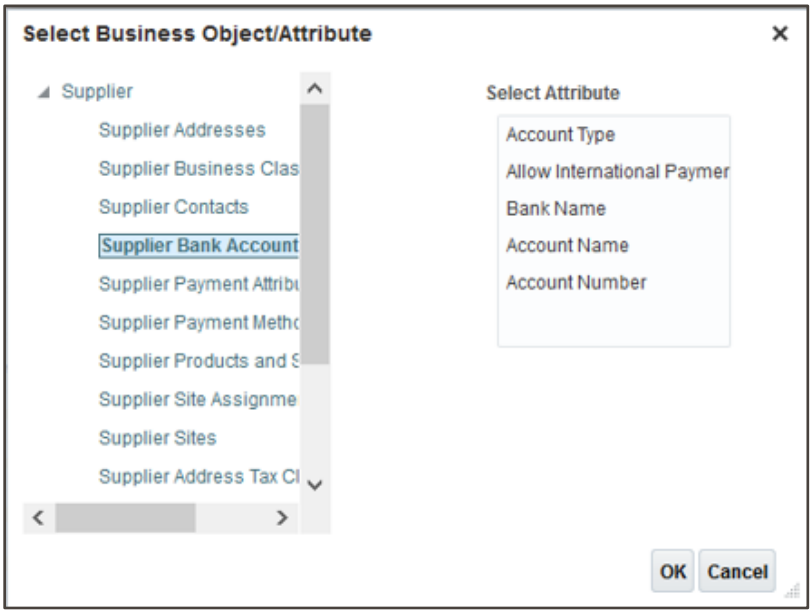
You can also select additional options above the result table headings, such as Show Attribute Details, select All Attributes, and Show additional object identifier columns.

Note: You can save your search criteria so you can easily return and review as business process owners enter changes to suppliers.



If you want to evaluate a specific attribute, instead of selecting ‘All Attributes’ above the result table headings, pick a specific attribute like Supplier Bank Account. Filter on the Supplier Bank Account to review only those events.





Continue to review audit changes, or make additional changes or additions to supplier and general ledger data in the development environment to have sufficient data to test going forward into next section.

Update and Test Configuration Models

Overview and Participants

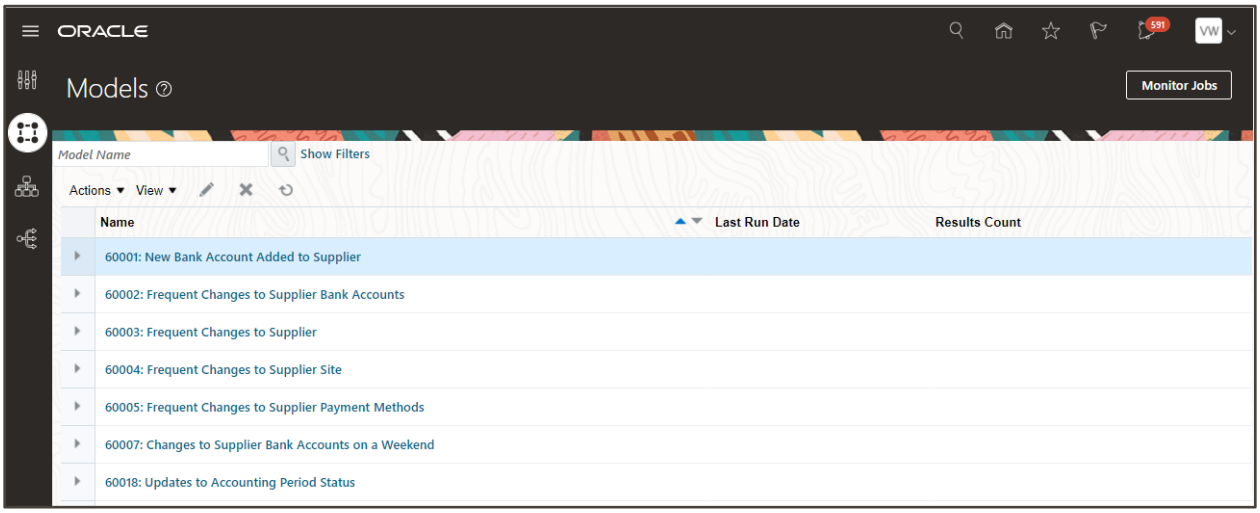
Your risk and compliance team will import and/or create models, deploy and manage configuration controls, and work together with business owners who may also manage controls and incident results. They are responsible for security assignment related to these areas.

Your ERP business process owners will be responsible for validating configuration 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.

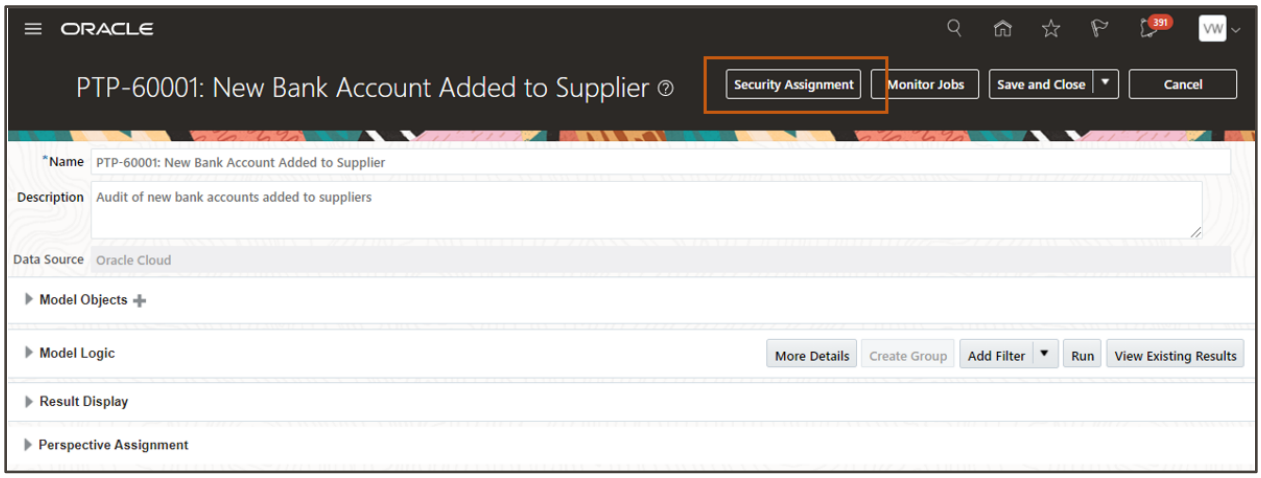
Step 1: Review and Update Security Assignments

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.

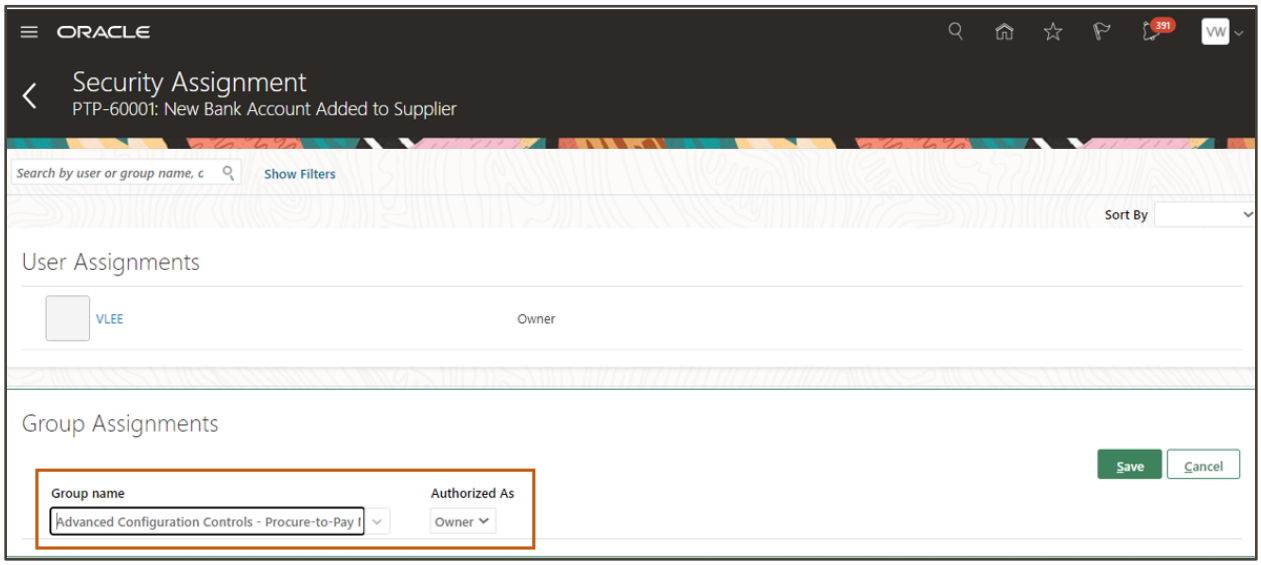
In Risk Management, navigate to Advanced Controls > Models to assign security authorization. Select the delivered model “60001: New Bank Account Added to Supplier”.



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 Configuration 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 then what you require in production.

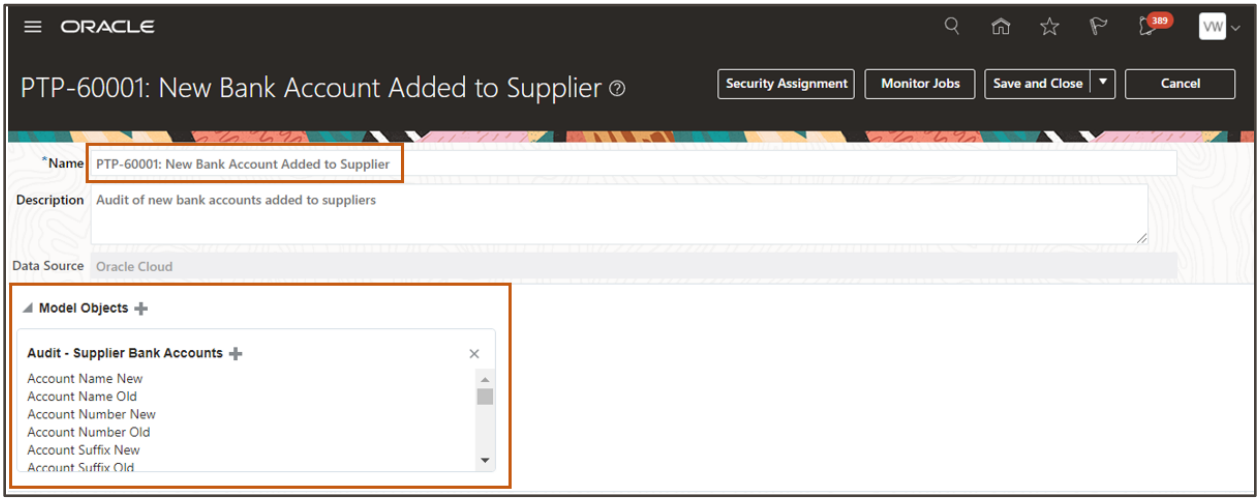
- Be sure to involve any other users to evaluate the results, or even those who need to add more test data by granting them access as at least a 'Viewer' of the model results (depending upon their role). Once a model is deployed as a control, you can no longer make changes to the logic or attribute columns 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 configuration controls and results tracked.

Note: Model results are considered temporary because each time you run the model the results are replaced. Once you deploy the model as a control, each record returned corresponds to a Result ID that cannot be deleted or replaced and provides an audit trial of every control incident result returned and tracked.

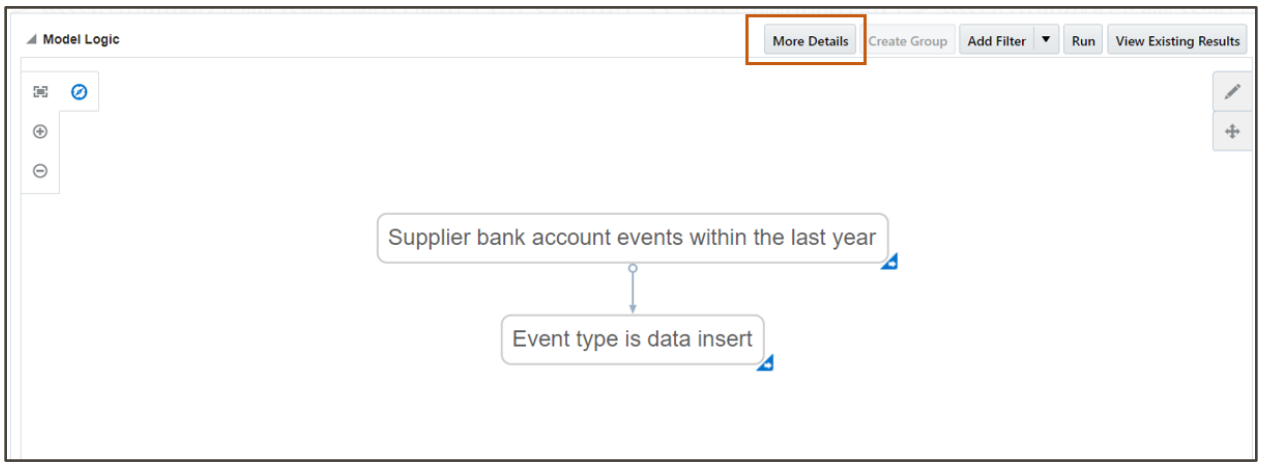
Overview of Model Definition

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.

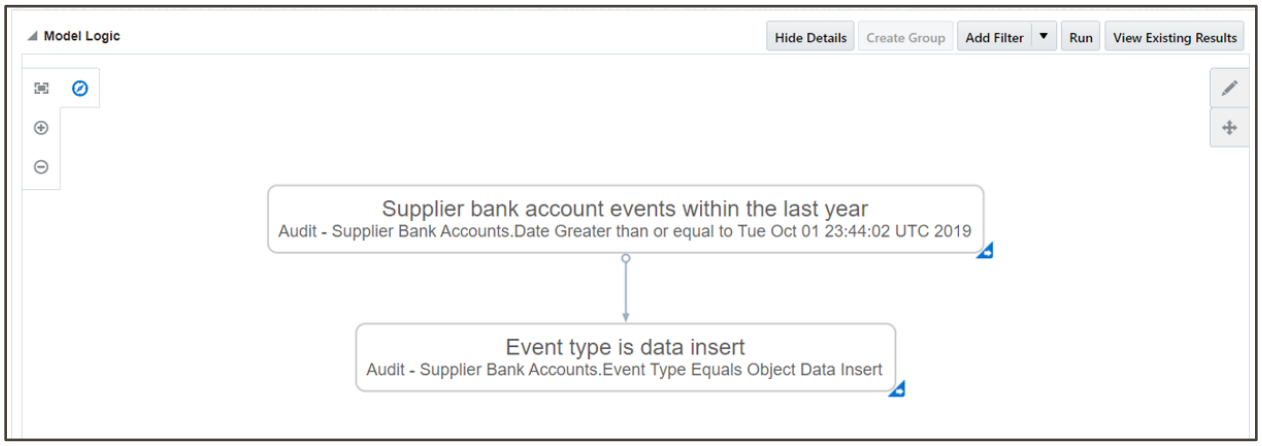


One of the most important sections of a model definition is the logic that provides the rules for incident to be returned and remediated after it is deployed as a control. To review additional Model Logic information, click on 'More Details' button in that region.

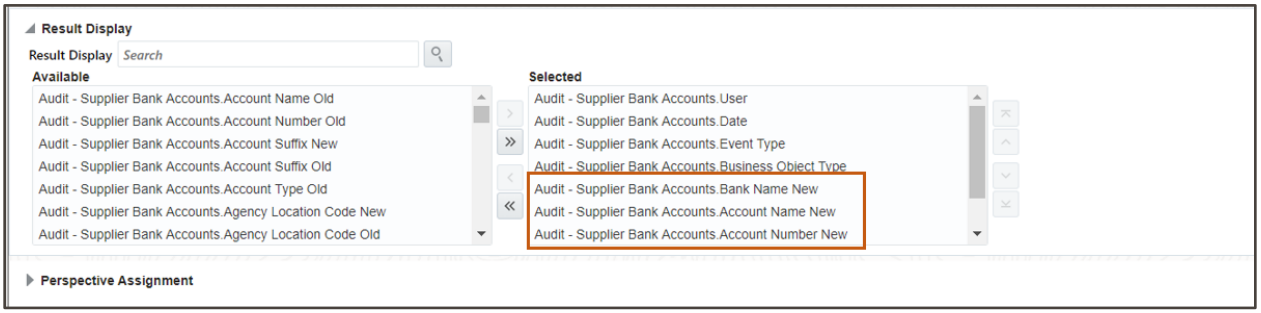


If you have owner or editor access, you can open the filter and edit the logic. This document uses the delivered models as-is. For example, this 60001 model includes two filters:

- First filter applies a date range for the configuration change of one year
- Second filter is looking for only 'insert' events



The Result Display section is where attributes are selected to be returned in results. As discussed earlier, the attributes that contain suffix of New or Old represent those business object attributes configured in Fusion Manage Audit Polices that are to be tracked.



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

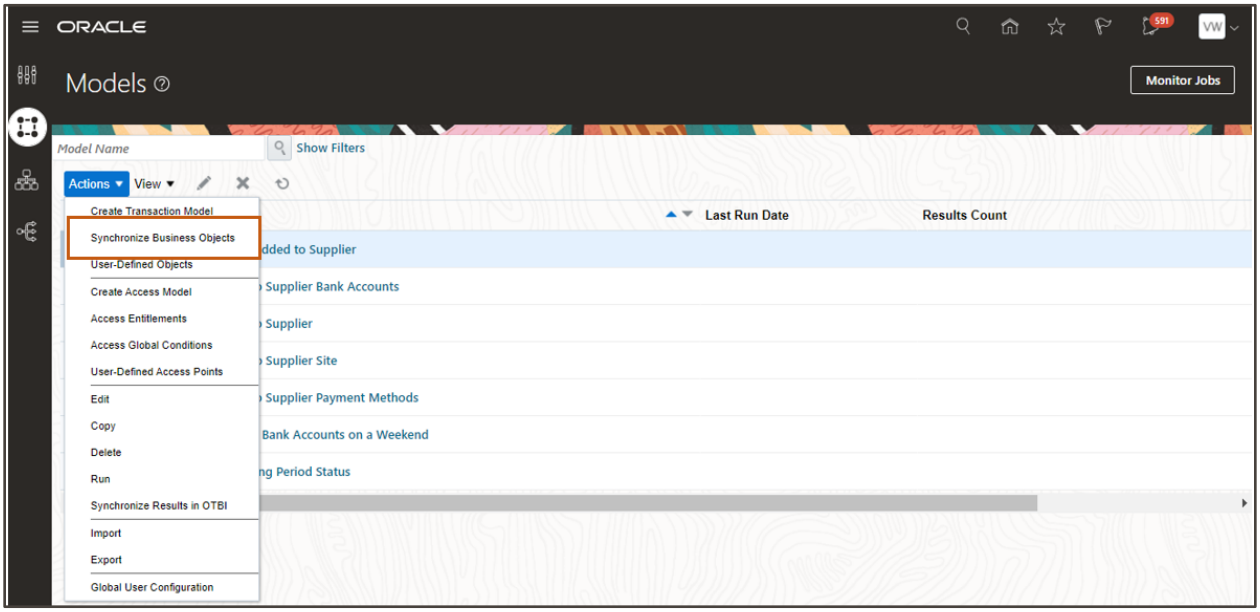
Note: For purposes of this document and any following steps around reporting, we use the delivered model logic and attribute definitions in model.

Step 2: Run Synchronization for a Model

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

Using model 60001 as an example to synchronize at the model level, select Actions > Synchronize Business Objects.

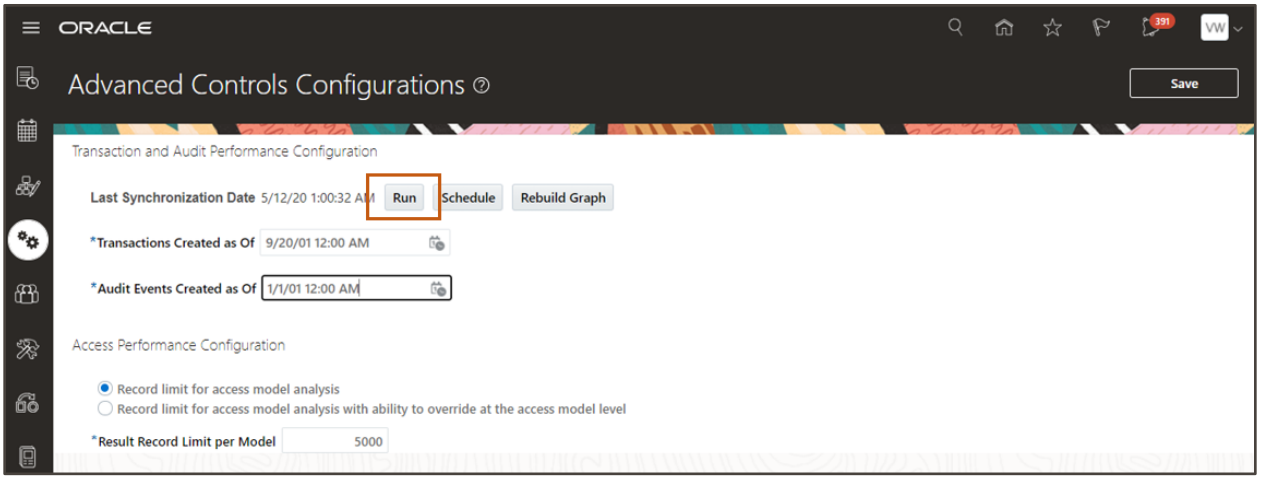
You can only use this option if the business object used in model has never been synchronized before; it does not apply to incremental updates. If previously synchronized, proceed to the next step.



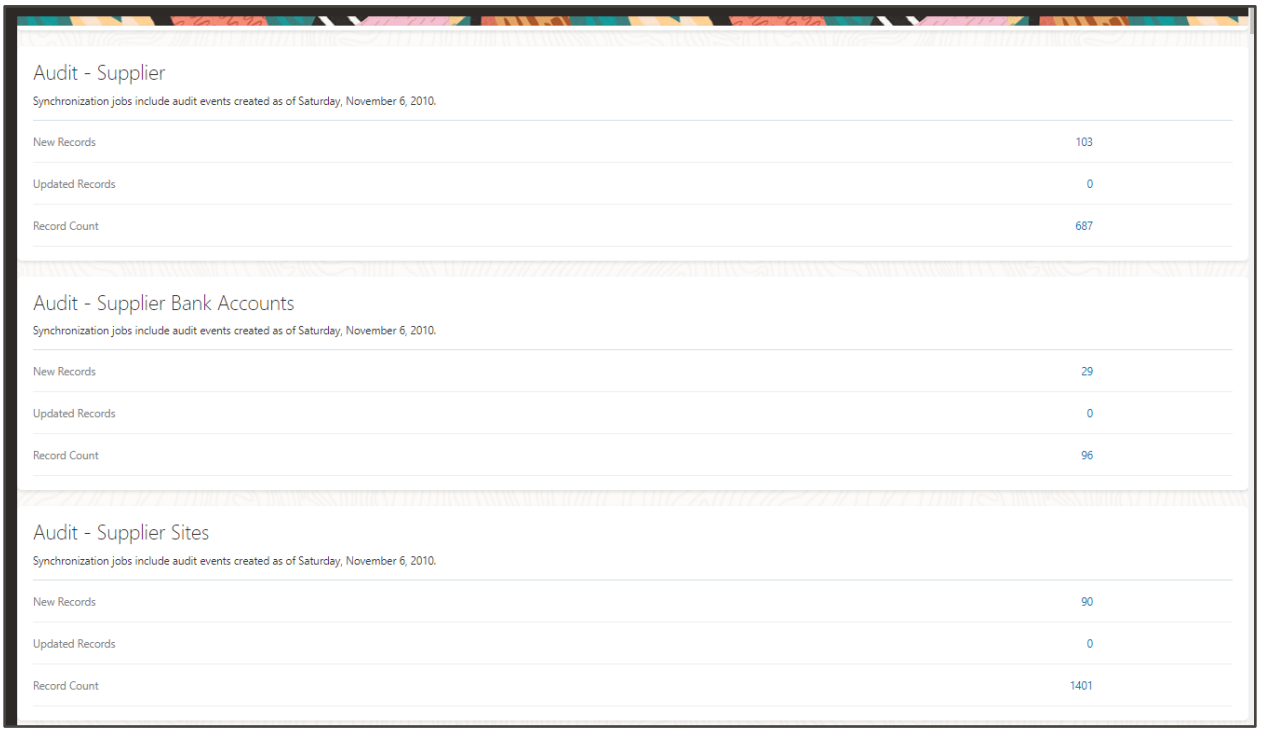
Step 3: Run Synchronization for All Business Objects

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 4: Run Model Results

Run each of the delivered models and review the data results. If there are some you did not get data for, or does not provide enough sample data, you will need to create some additional test data in your development environment. You would follow these steps in document:

1. Go back to Audit Policy Prerequisite Steps, refer to Steps 5 and 6 to create configuration test data.
2. After configuration changes are made, you need to run transaction synchronization again to update event records for a business object used (previous Step 3).

Deploy and Run Configuration Controls

Overview and Participants

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

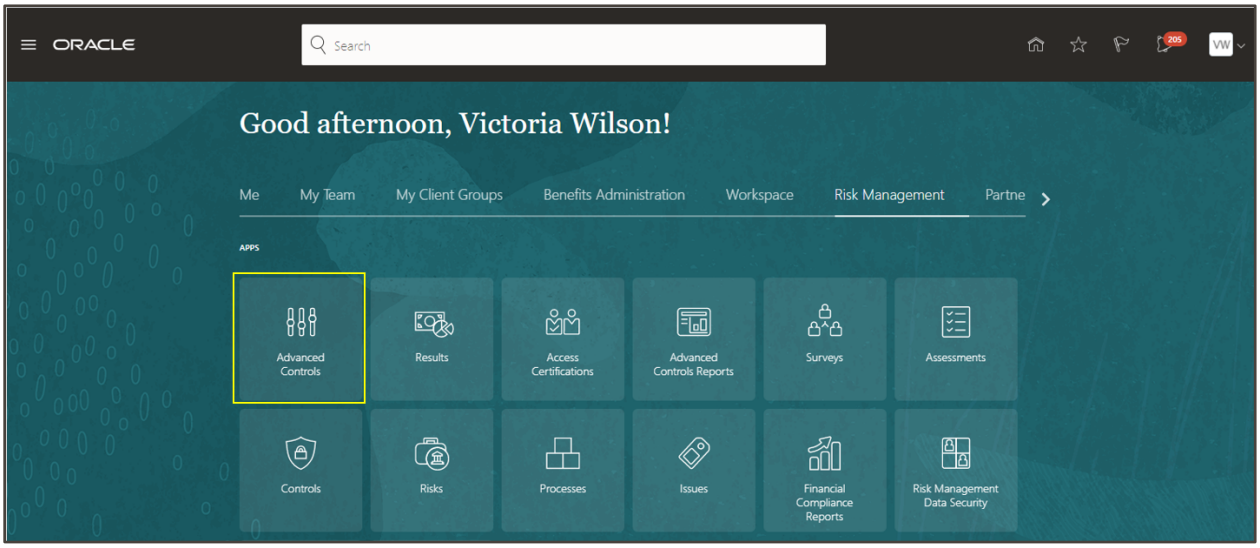
Your ERP business process owners will be responsible for validating configuration controls and the incidents they return. They typically are the ones signing off on controls to promote to production, and finalizing security assignment responsibility related to these areas.

Step 1: Deploy Configuration Controls

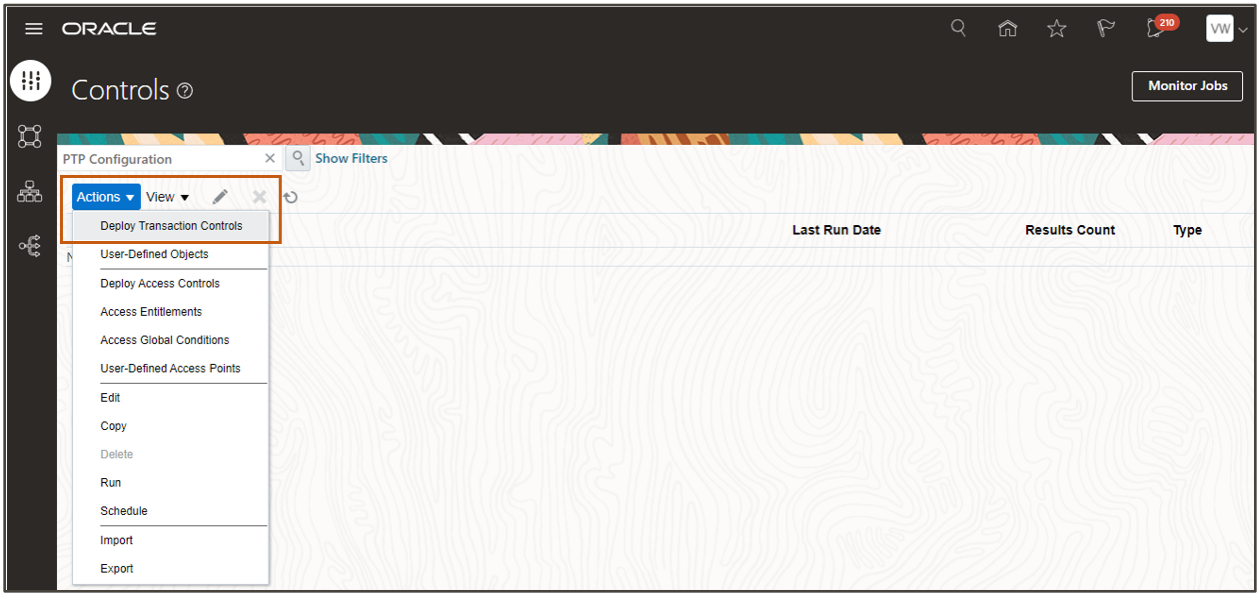
Based on collaboration between your risk and compliance team, and the business process owners input, deploy models as controls to test continuously monitored configuration events in development and eventually production.

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 configuration 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 configuration controls, navigate to Risk Management > Advanced Controls.



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

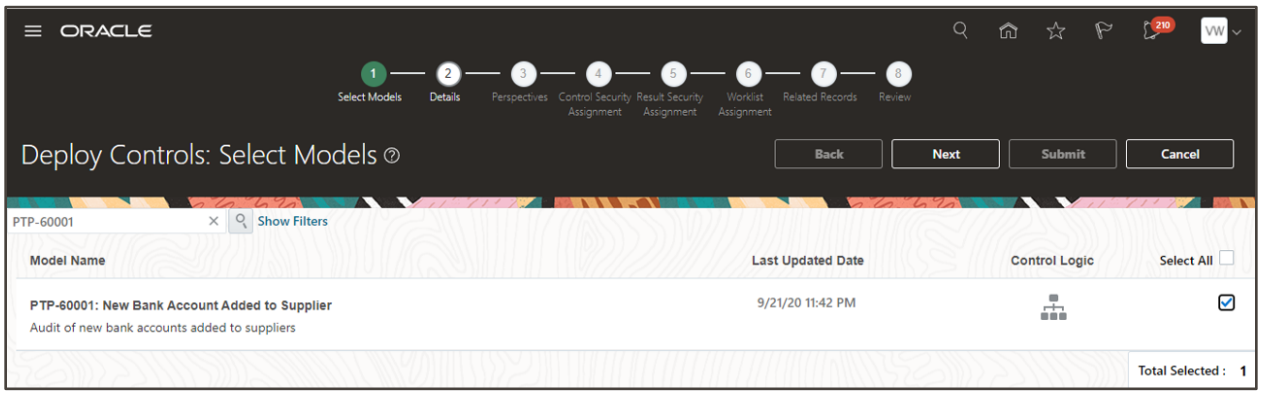


The following sections cover each of the train stops – or page - to select and deploy configuration controls.

Select Models

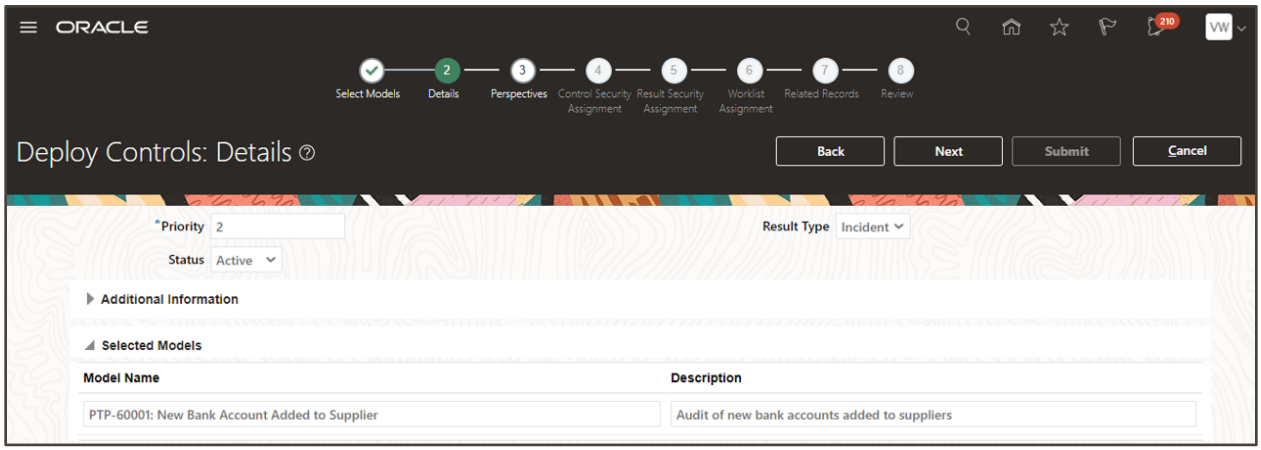
Select from an available list of transactions models to create controls. In line with previous steps, search and select those seven PTP and RTR configuration models covered in document. You can select one at a time to create a control when criteria differs, such as priority or user assignment groups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

The following examples uses one model as an example to deploy as a control: 60001: New Bank Account Added to Supplier. Select Next to proceed.



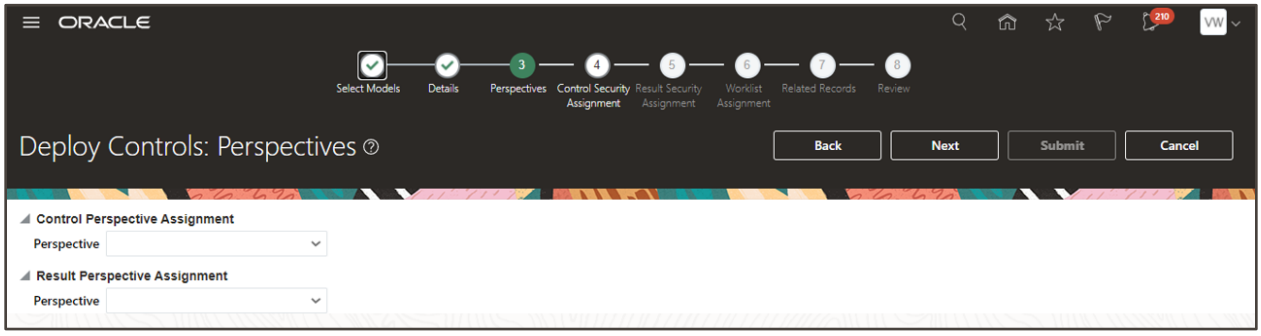
Details

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.

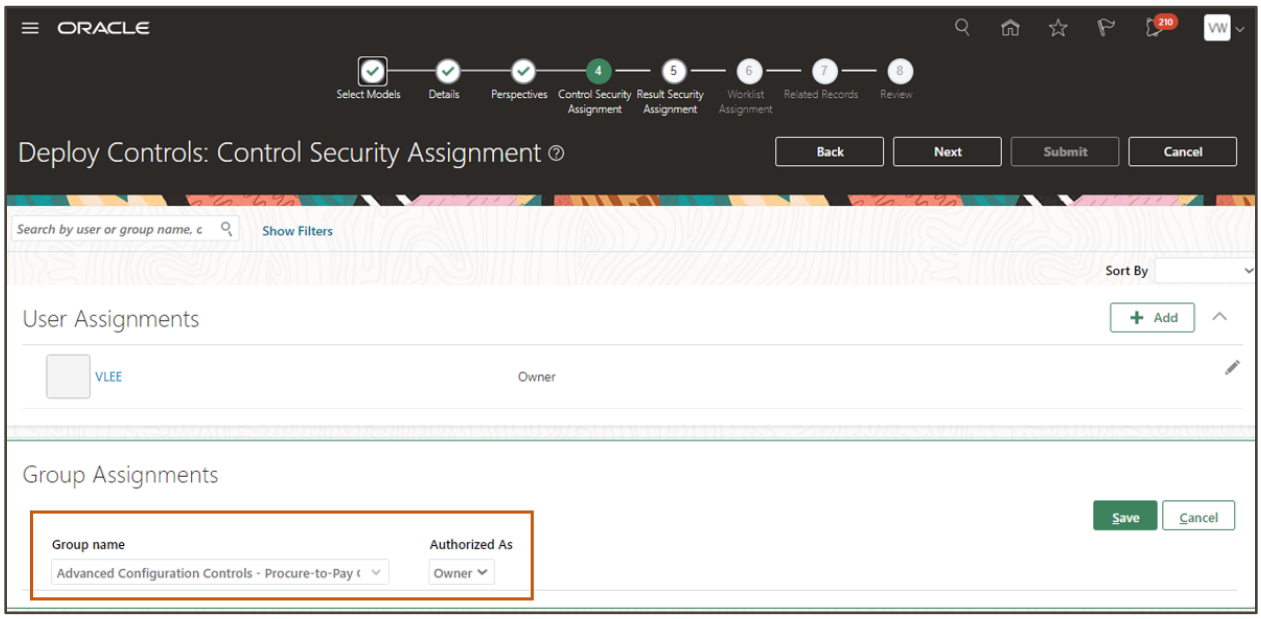


Control Security Assigment

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.

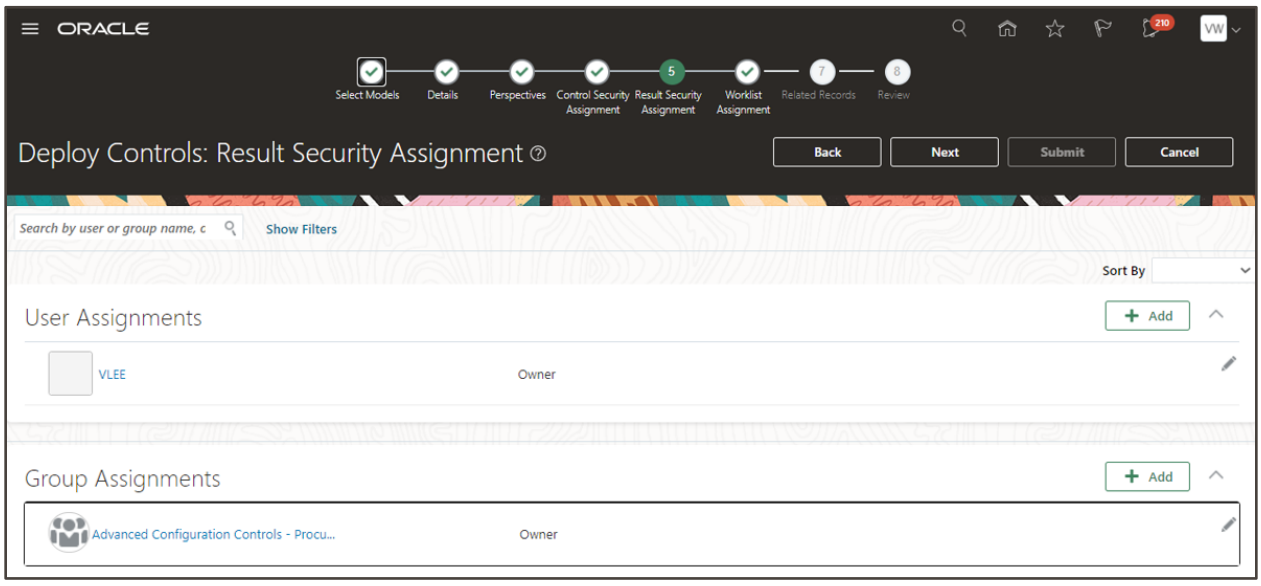


Result Security Assignment

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.

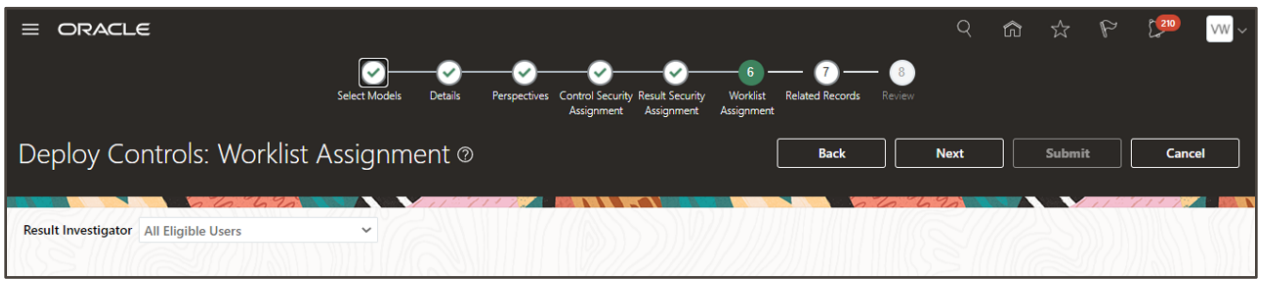
After selecting Save, select Next to proceed.



Worklist Assignment

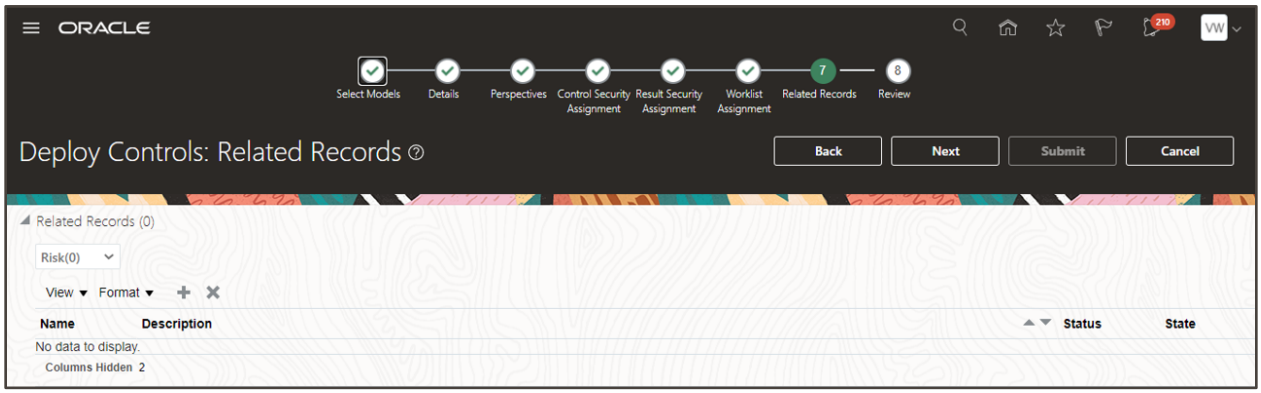
On the Worklist Assignment page you can leave the default to include All Eligible Users to receive a worklist, or assign one user as the primary result investigator. In this case, even though one user may receive the worklist, any user authorized to own or edit can access and update the incidents.

Select Next to proceed.



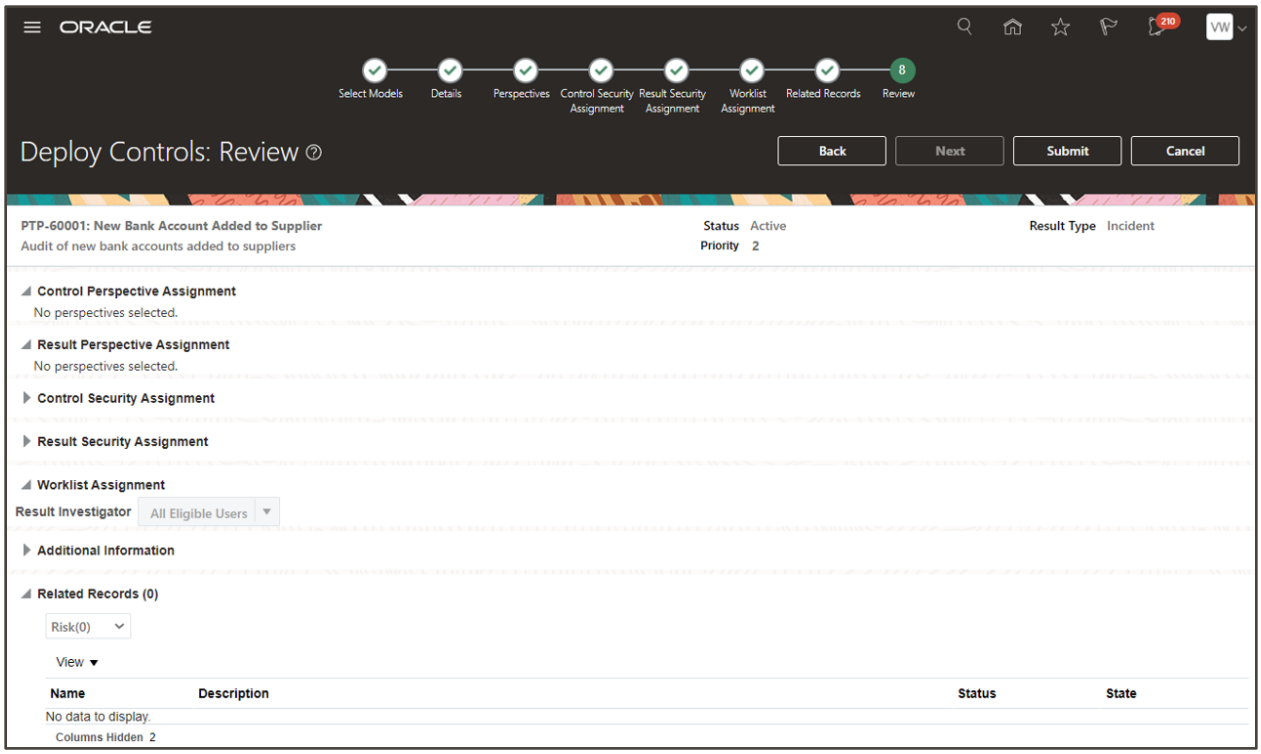
Related Records

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.

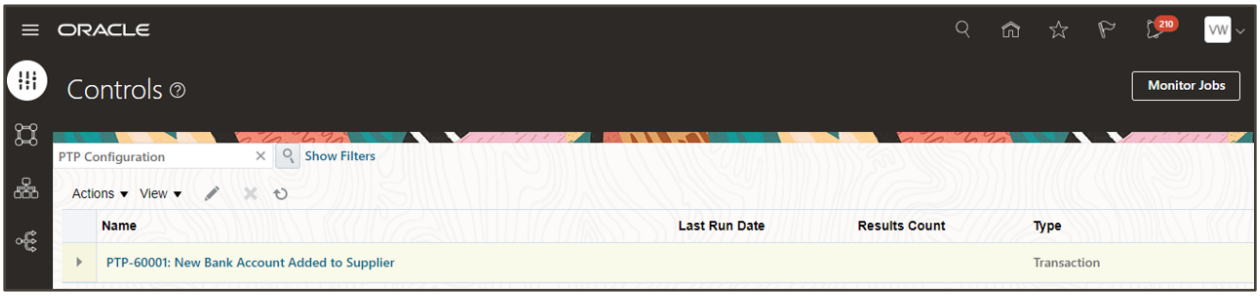


Review

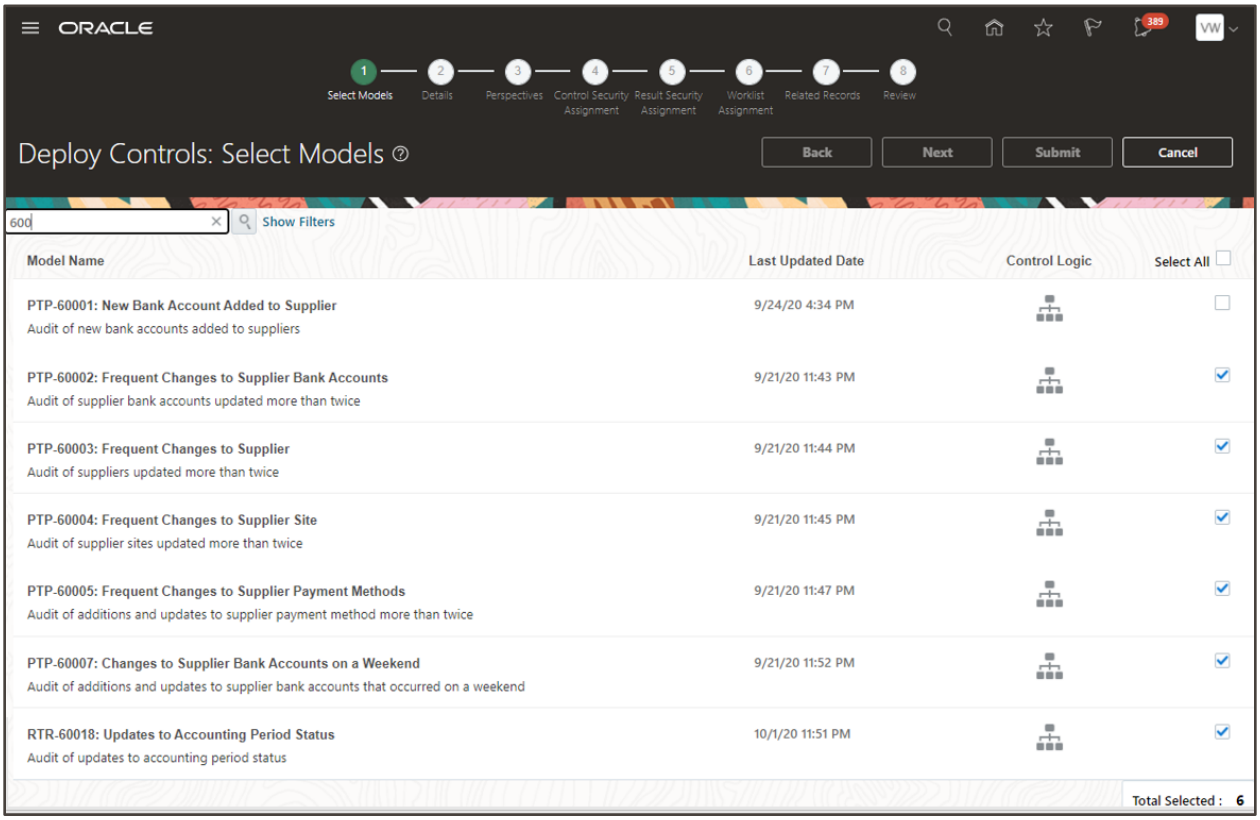
The last Review page to deploy a control provides an overview of all the criteria set; if satisfied, select the Submit button.



Your selected model has now been deployed as a control.



Using these steps, go back and deploy the remaining six models as control. 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.

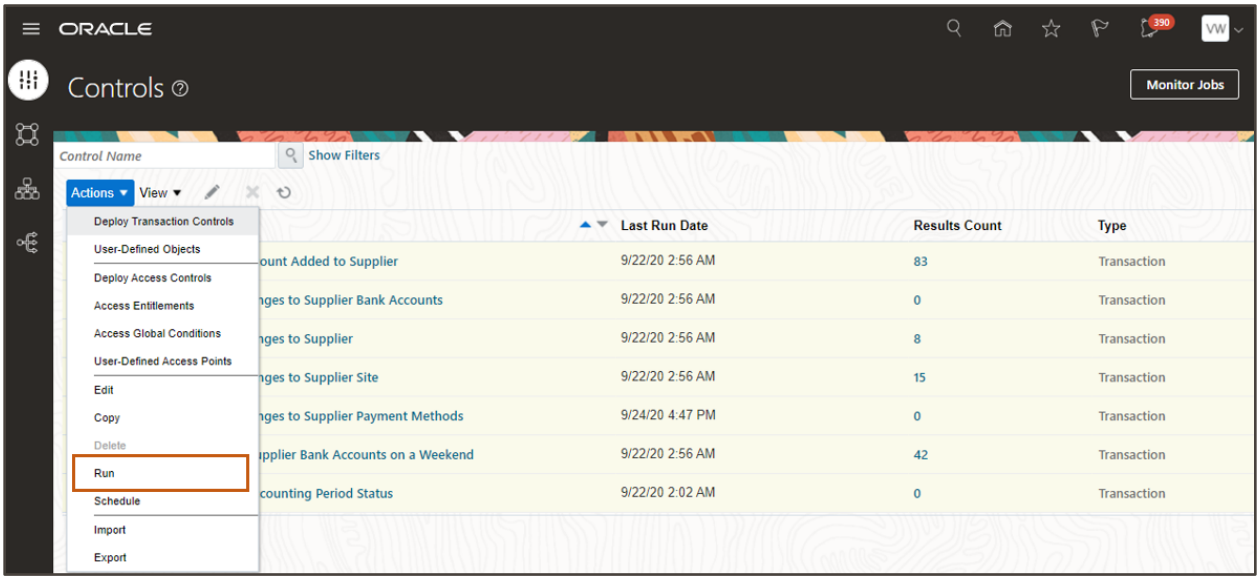


Step 2: Run Data Synchronization

Before running control analysis on your configuration 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

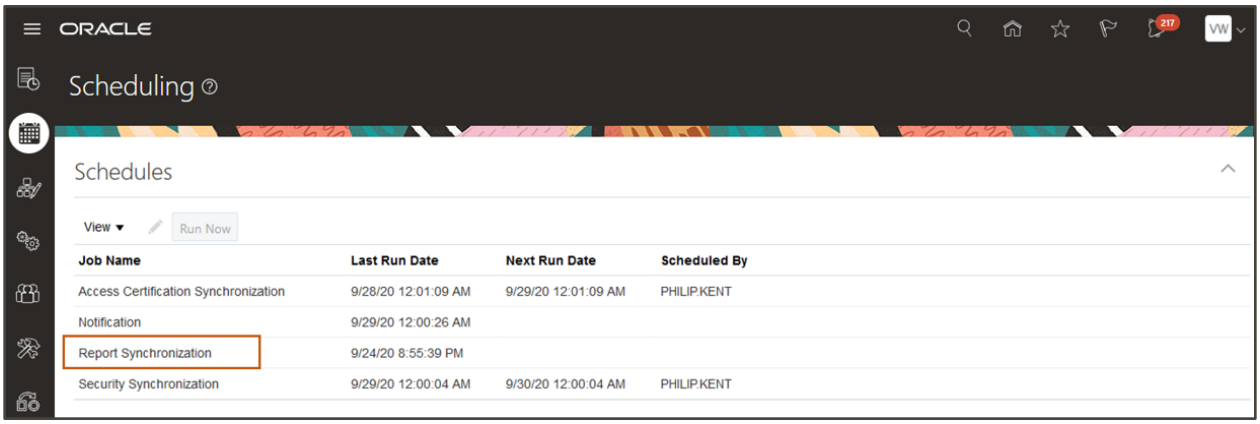
Once the synchronization job is complete, navigate to Risk Management > Advanced Controls to run control analysis. Select one to many controls, then select Actions > Run from the toolbar.



Step 4: Run Report Synchronization

After all your configuration controls have completed, you now run the Report Synchronization job. This job makes the data available in OTBI subject areas used by dashboards and reports. The configuration 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.

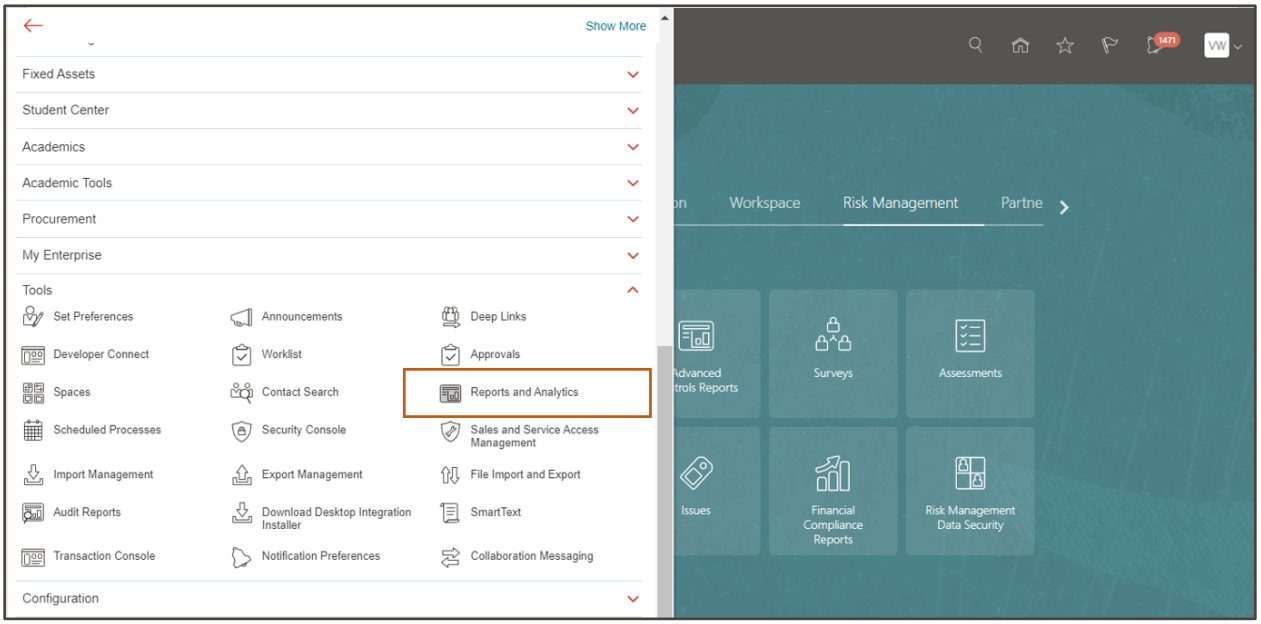
Your ERP business process owners will use these reports and dashboards to evaluate and remediate incident results for configuration controls.

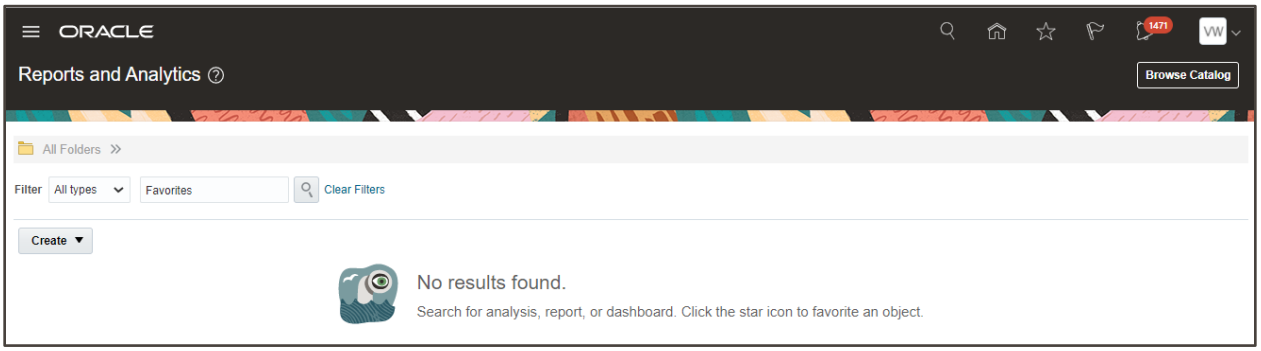
Step 1: Unarchive Risk Management Dashboard

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 above website to update artifacts related to Configuration Controls under the '00 Dashboard' and '50 Monitor Configurations', 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.

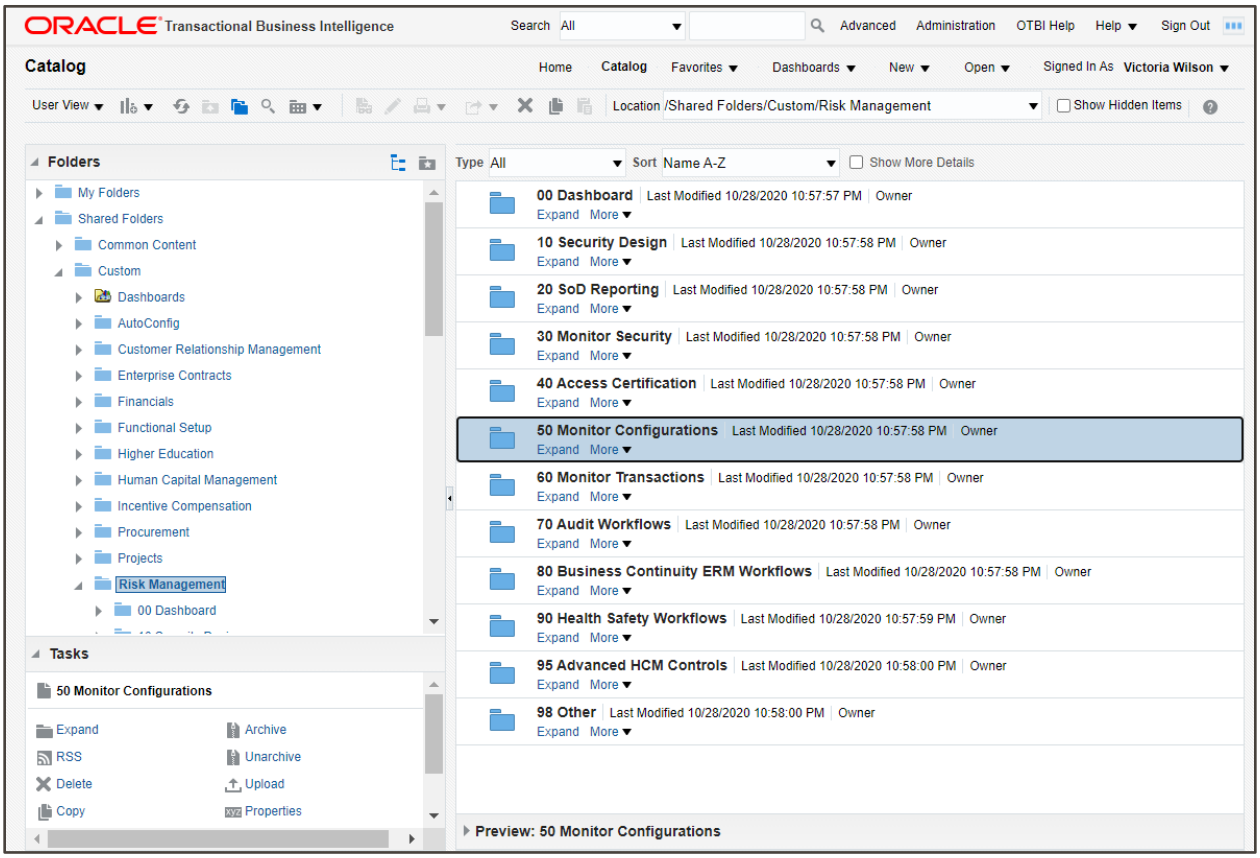
Navigate to Reports and Analytics, and then select Browse Catalog.





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.

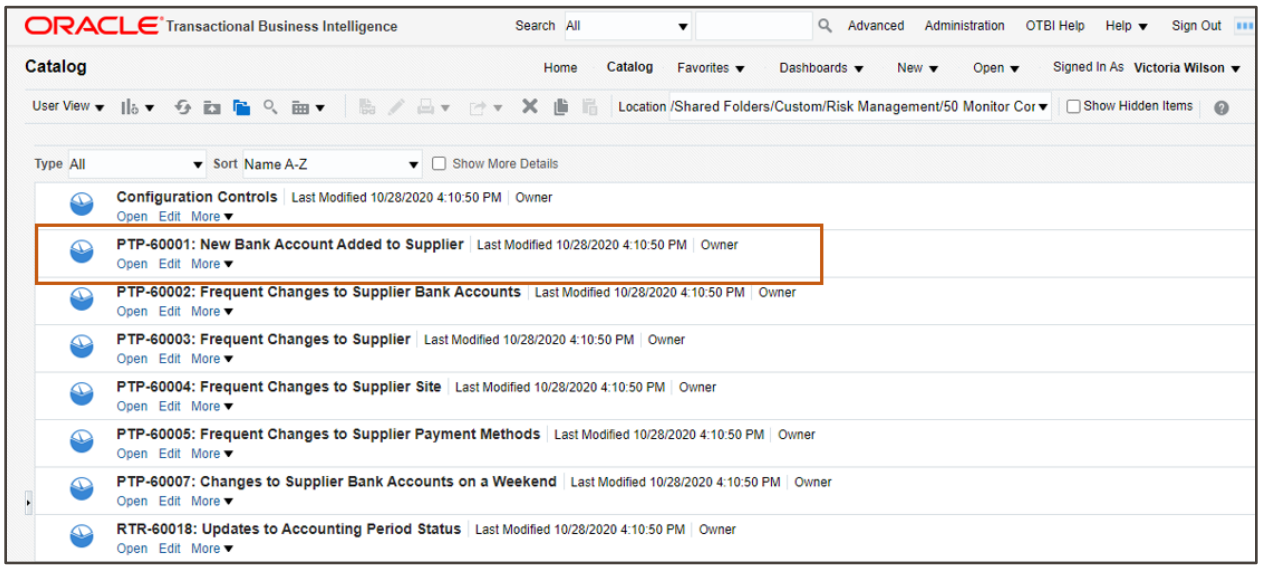
Subsequent steps will show you how to update reports under the '50 Monitor Configurations' folder.



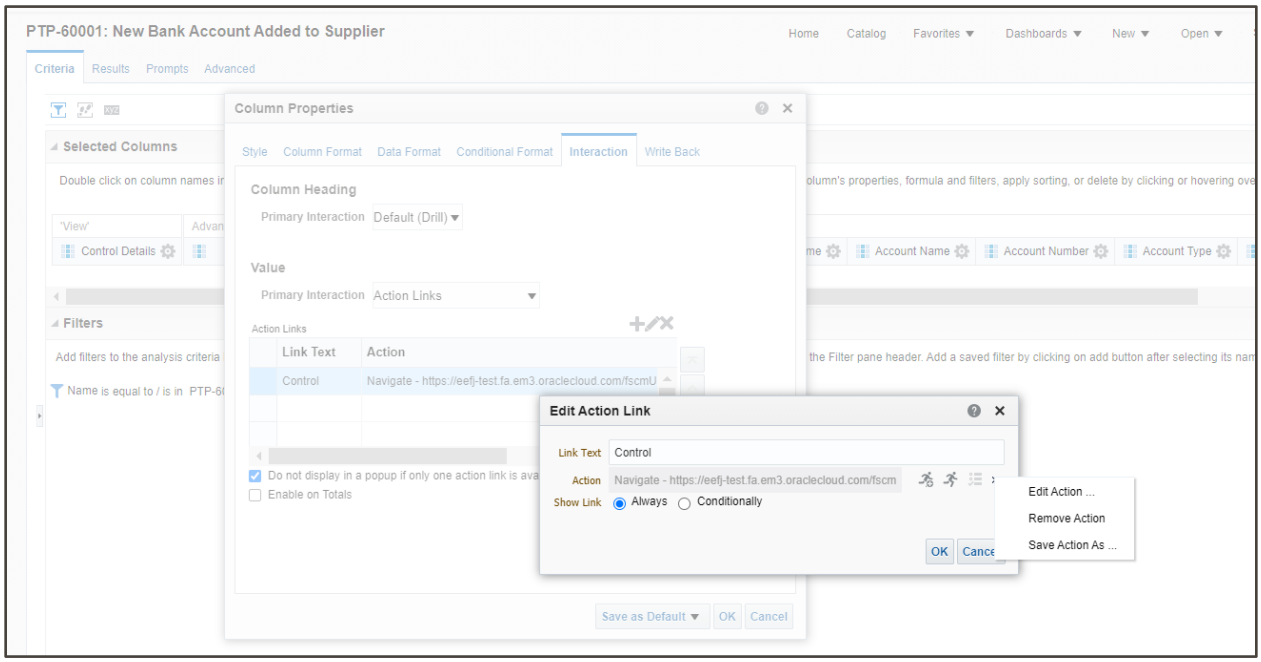
Step 2: Update Each Control Detail Report

With your Risk Management Dashboard in place, you will need to update URL deep links with the host/environment name for reports under folder '50 Monitor Configurations'. 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-60001: New Bank Account Added to Supplier", and go to the Criteria page.

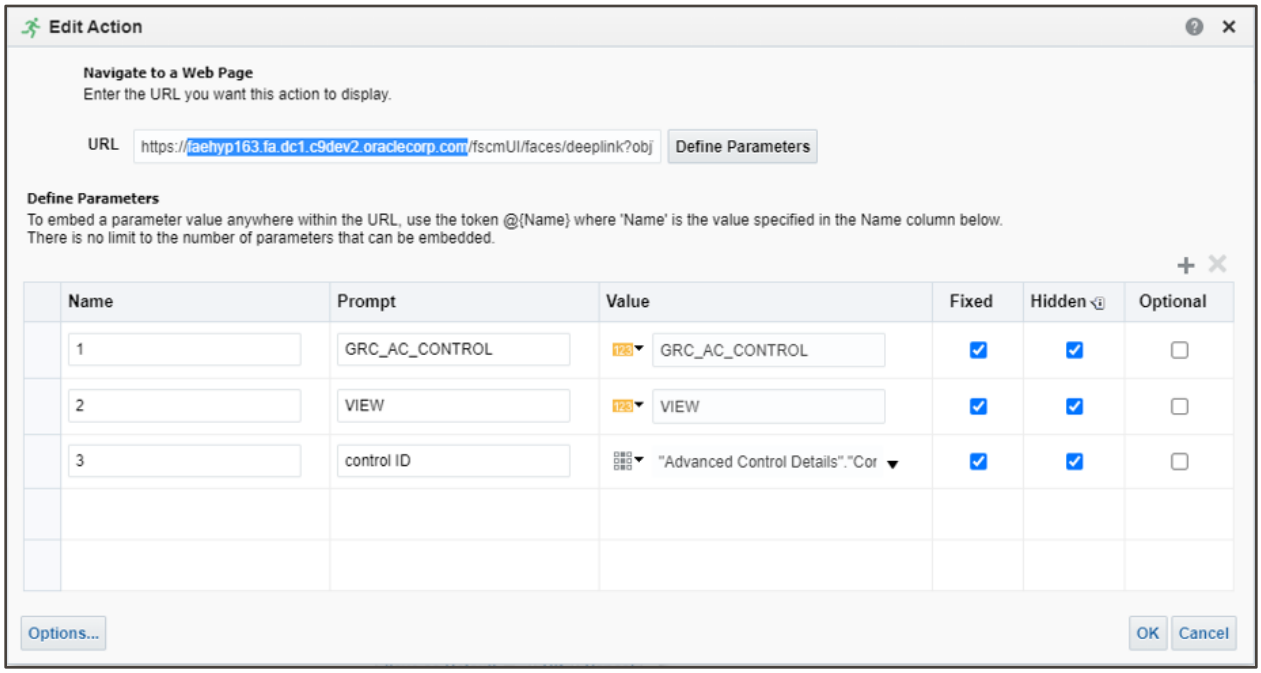


For the ‘Control Details’ column, select the gear box icon then Interaction tab. Highlight the Action Link for control on tab, Edit icon, and Edit Action.

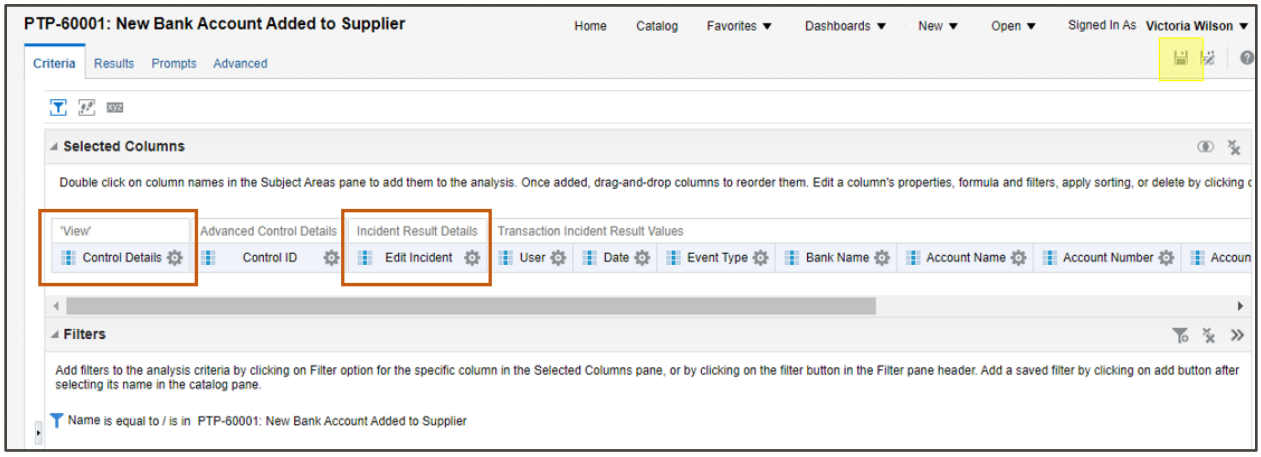


On the Edit Action page, update the URL host name that corresponds to your development environment (see the highlighted section in URL below).

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 ‘50 Monitor Configurations’.



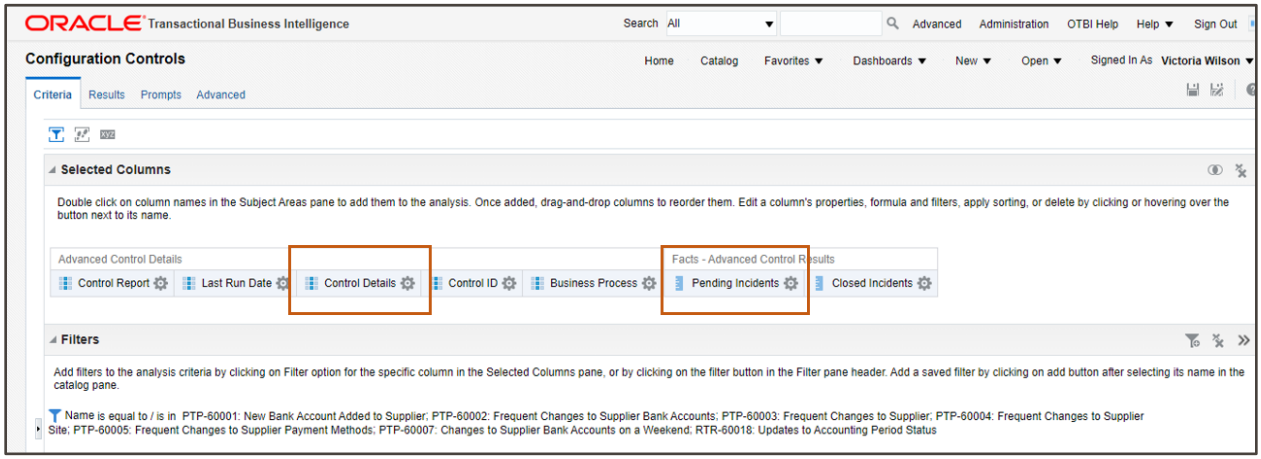
Perform the same steps for all control reports in this folder, updating the URL for deep links for ‘Control Details’ and ‘Edit Incident’ columns. All these control detail reports contain these two columns:

- PTP-60001: New Bank Account Added to Supplier
- PTP-60002: Frequent Changes to Supplier Bank Accounts
- PTP-60003: Frequent Changes to Supplier
- PTP-60004: Frequent Changes to Supplier Site
- PTP-60005: Frequent Changes to Supplier Payment Methods
- PTP-60007: Changes to Supplier Bank Accounts on a Weekend
- RTR-60018: Updates to Accounting Period Status

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’50 Monitor Configurations’.

Step 3: Update Configuration Controls Report

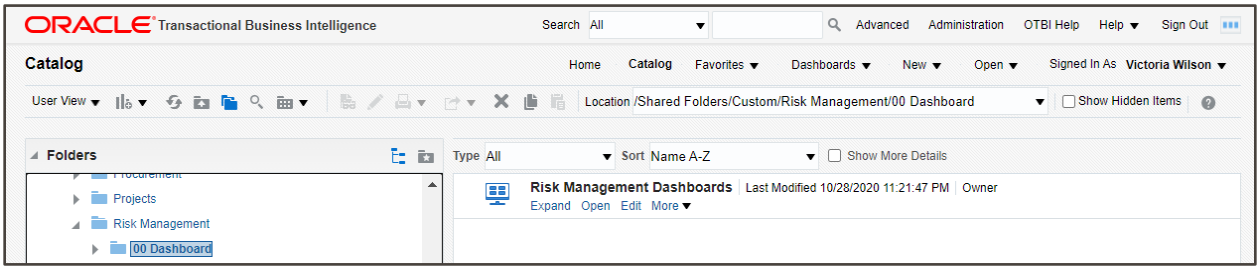
Similar to prior steps for control detail reports, the "Configuration Controls" report used in the dashboard also requires updating to columns using your environment URL host for deep links. Edit the action links for 'Control Details' and 'Pending Incidents' columns, just as described in the previous step. Save the report and return to the '50 Monitor Configurations' catalog folder.



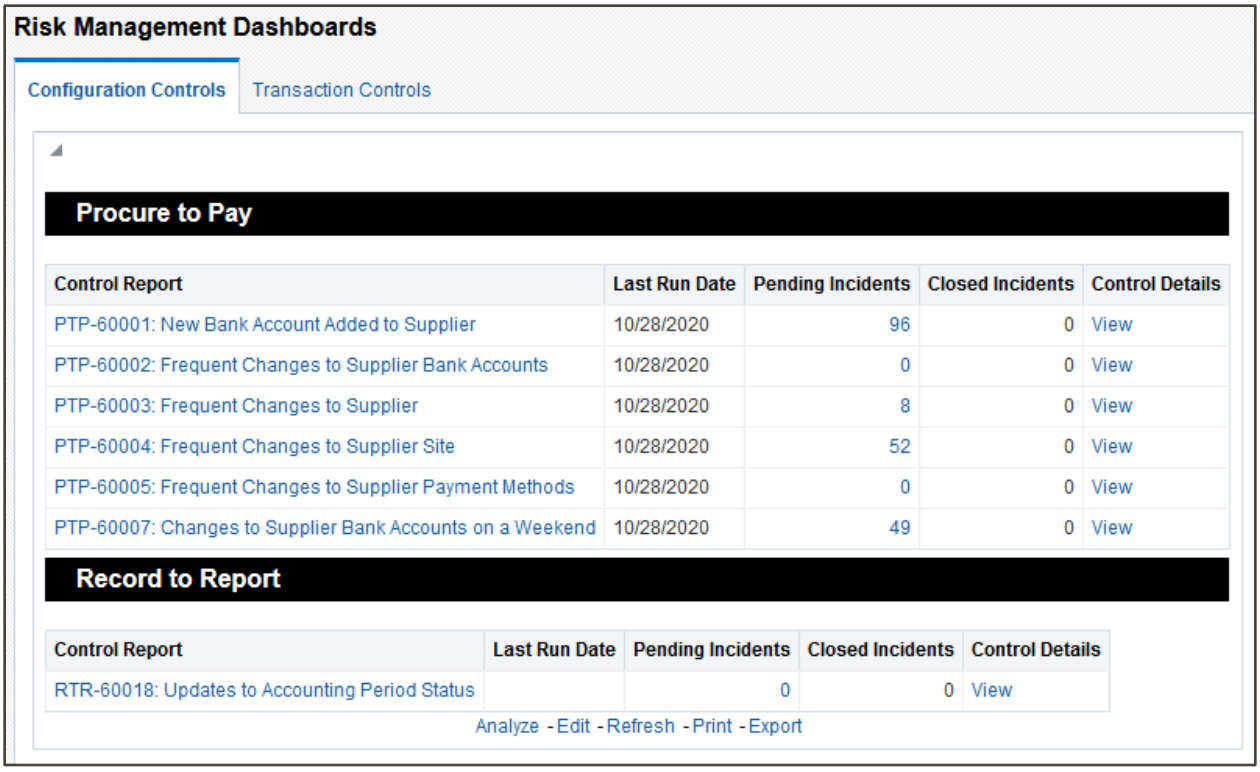
Note: A deep drill on the Closed Incidents column is not currently supported.

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 Configuration 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.



Risk Management Dashboards

Configuration Controls | Transaction Controls

Procure to Pay

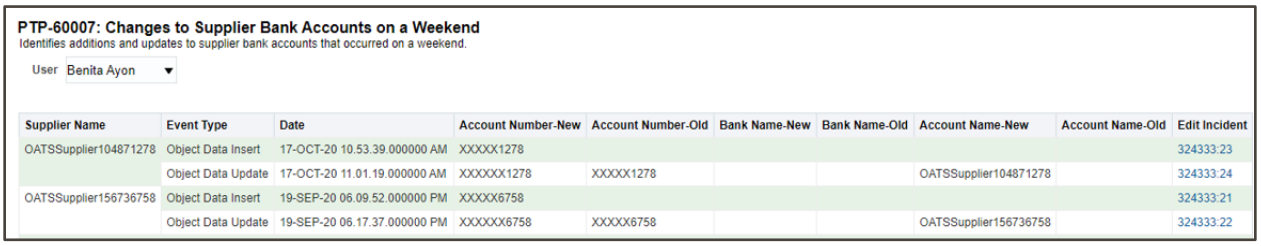
Control Report	Last Run Date	Pending Incidents	Closed Incidents	Control Details
PTP-60001: New Bank Account Added to Supplier	10/28/2020	96	0	View
PTP-60002: Frequent Changes to Supplier Bank Accounts	10/28/2020	0	0	View
PTP-60003: Frequent Changes to Supplier	10/28/2020	8	0	View
PTP-60004: Frequent Changes to Supplier Site	10/28/2020	52	0	View
PTP-60005: Frequent Changes to Supplier Payment Methods	10/28/2020	0	0	View
PTP-60007: Changes to Supplier Bank Accounts on a Weekend	10/28/2020	49	0	View

Record to Report

Control Report	Last Run Date	Pending Incidents	Closed Incidents	Control Details
RTR-60018: Updates to Accounting Period Status		0	0	View

Analyze - Edit - Refresh - Print - Export

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.



PTP-60007: Changes to Supplier Bank Accounts on a Weekend

Identifies additions and updates to supplier bank accounts that occurred on a weekend.

User Benita Ayon

Supplier Name	Event Type	Date	Account Number-New	Account Number-Old	Bank Name-New	Bank Name-Old	Account Name-New	Account Name-Old	Edit Incident
OATSSupplier104871278	Object Data Insert	17-OCT-20 10.53.39.000000 AM	XXXXX1278						324333:23
	Object Data Update	17-OCT-20 11.01.19.000000 AM	XXXXXX1278	XXXXX1278			OATSSupplier104871278		324333:24
OATSSupplier156736758	Object Data Insert	19-SEP-20 06.09.52.000000 PM	XXXXX6758						324333:21
	Object Data Update	19-SEP-20 06.17.37.000000 PM	XXXXXX6758	XXXXX6758			OATSSupplier156736758		324333:22

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 either prefix it with "PTP-" or "RTR-". This has a direct impact on using the Configuration Controls dashboard (organized by business process) delivered on Customer Connect.

Evaluating and Closing Incident Results

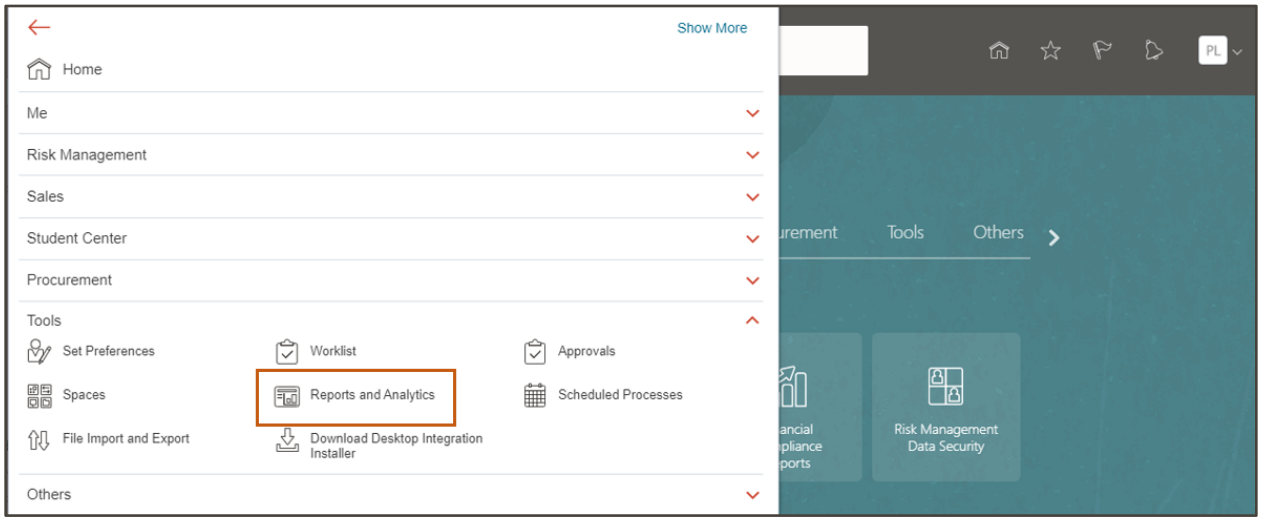
Overview and Participants

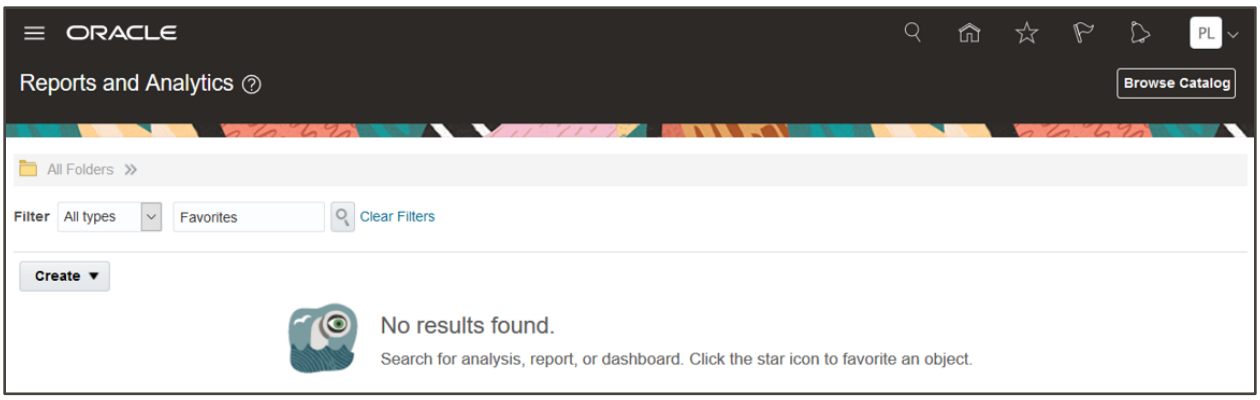
Your risk and compliance team supports business process owners in their review of controls and remediation of incidents. If additional users or security updates are required, they will work with the security team.

Your ERP business process owners will be responsible for validating configuration 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.

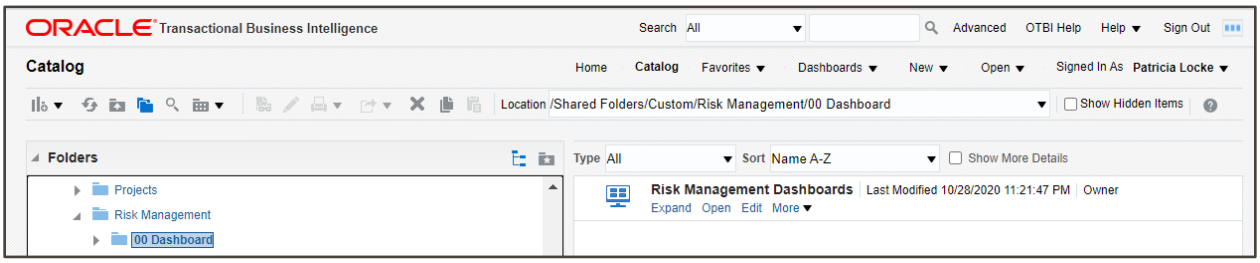
Step 1: Review Risk Management Dashboard

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.

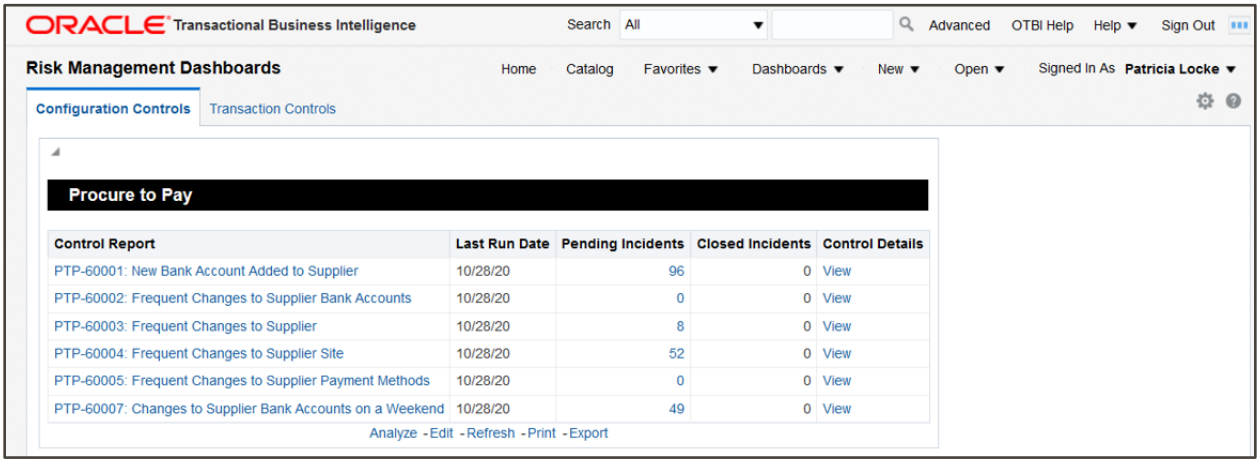




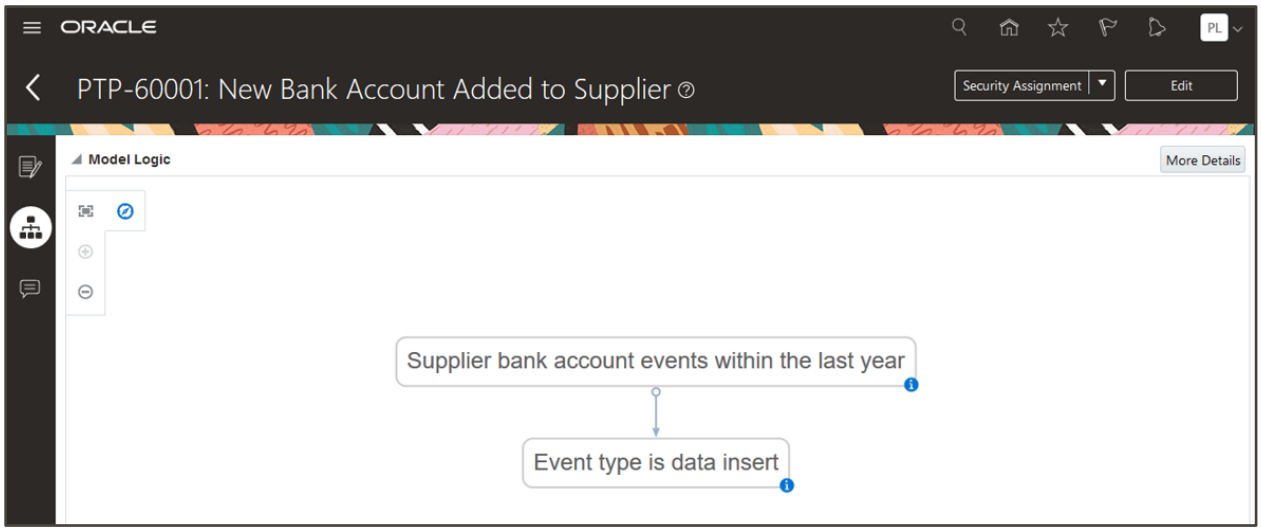
Go to folder Shared Folders > Custom > Risk Management > 00 Dashboard folder, and Open the Risk Management Dashboards.



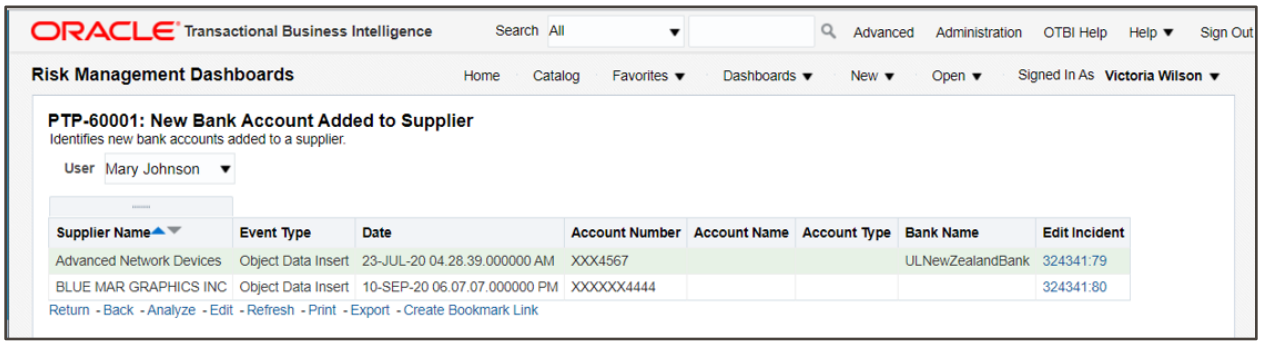
Select the Configuration Controls page in dashboard to review reports. This business user has access to the procure-to-pay control reports, and corresponding incidents and control details.



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 "PTP-60001: New Bank Account Added to Supplier".

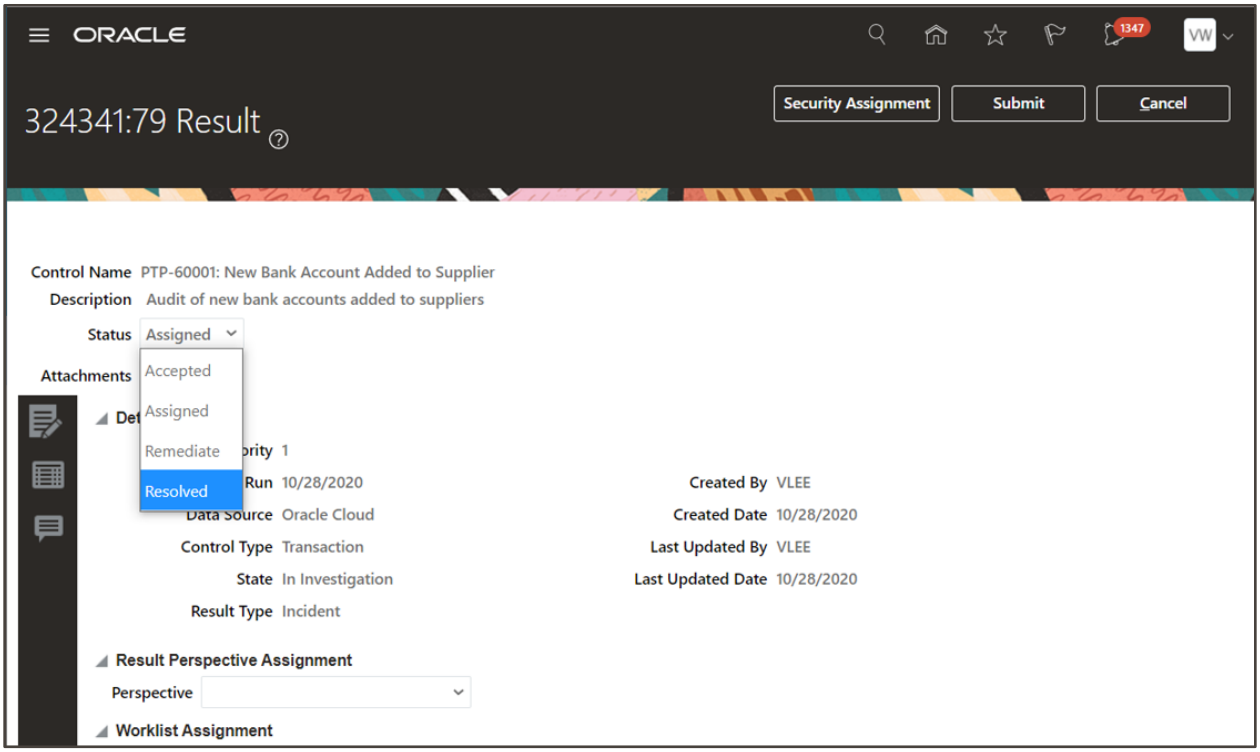


Each control report will vary, and corresponding incident results can be investigated and updated individually or in mass.

Step 2: Edit an Incident Result

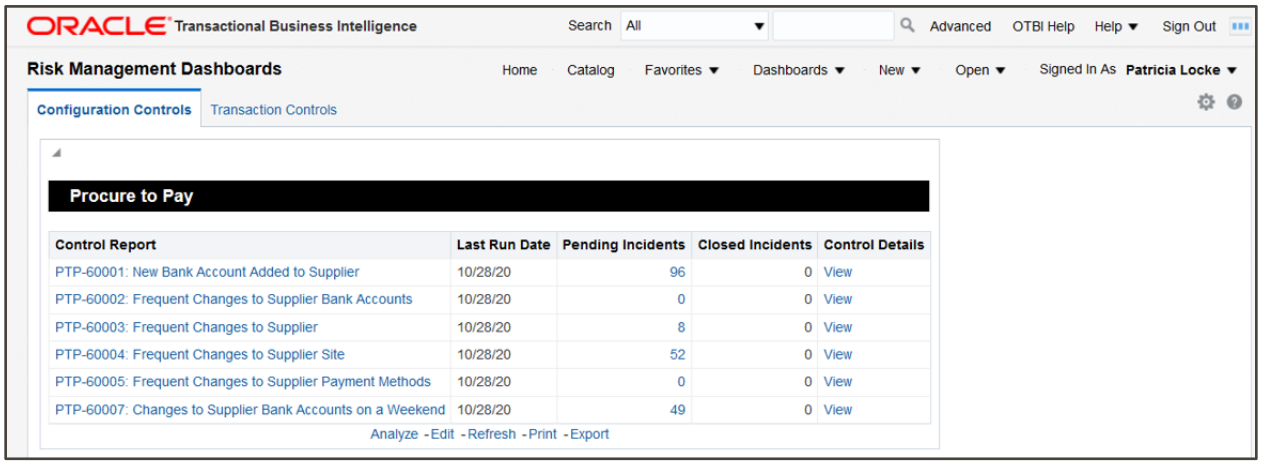
In each of the control report details, you will find a column called ‘Edit Incident’. Select a link at the row level to update an individual incident result.

Here is an example of opening a Result ID in Risk Management from report “PTP-60001: New Bank Account Added to Supplier”. A new window is opened for the Result ID and you can directly update the Status, add Attachments or Comments.



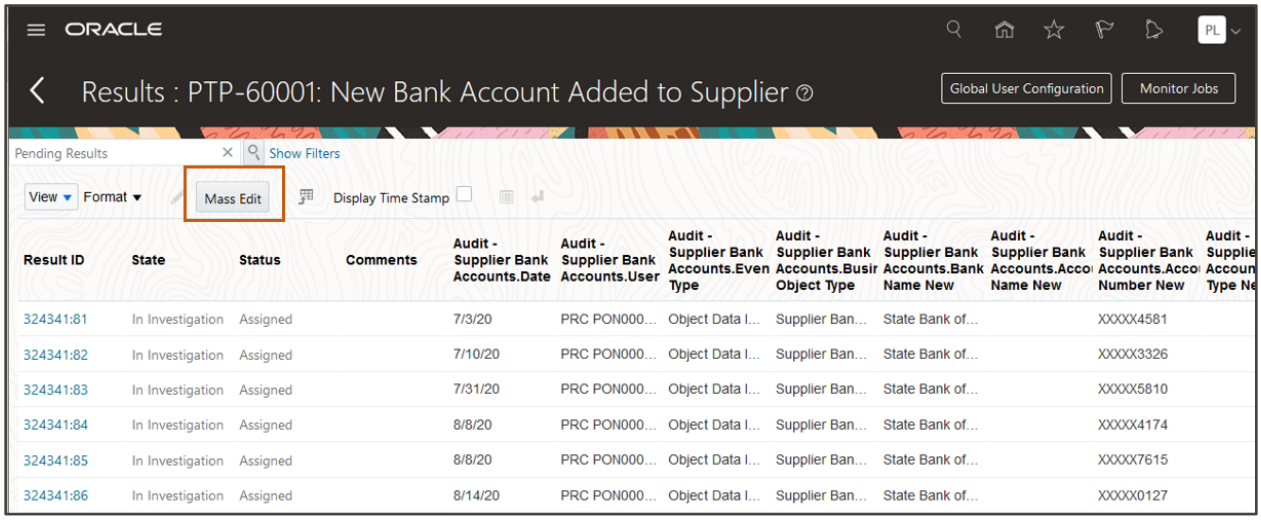
Step 3: Mass Edit Incident Results

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

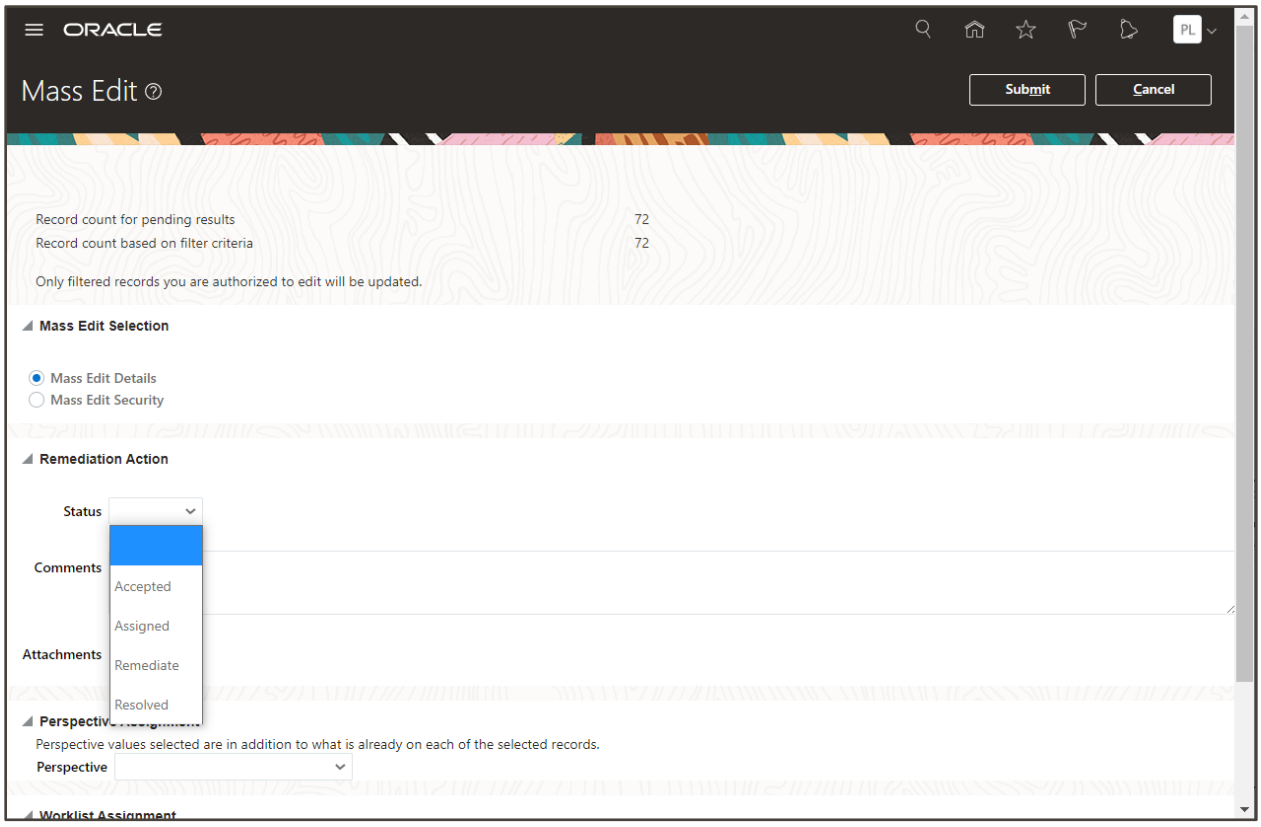


The Pending Incidents are returned for the control selected. Optionally, you can apply additional filters by applying criteria after opening Show Filters.

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. (The exception, you would not apply test data as indicated in Step 5: Enter Some 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.

BEST PRACTICE CONTENT LIBRARY

The following table provides the list of ERP Advanced Audit Controls library models you should apply; these are the seven covered in this document. The table includes the following information:

- Name of the model delivered in content library.
- Product area associated to business object and model that needs to be enabled under Fusion Manage Audit Policies.
- Name of the business object that corresponds to the Audit Policy (excluding the 'Audit –' prefix), and the matching business object found in advanced controls that does use the 'Audit – ' prefix.
- Attributes you must enabled for the business object under Fusion Manage Audit Policies; these attributes are those used in the delivered model content.

Model Name in ERP Content Library	Product (Audit Policy)	Business Object	Attributes
60001: New Bank Account Added to Supplier	Supplier Model	Audit - Supplier Bank Accounts	• Account Name • Account Number • Account Type • Bank Name
60002: Frequent Changes to Supplier Bank Accounts	Supplier Model	Audit - Supplier Bank Accounts	• Account Name • Account Number • Account Type • Allow International Payments • Bank Name
60003: Frequent Changes to Supplier	Supplier Model	Audit - Supplier	• Inactive Date • One-time Supplier • Supplier Type • Tax Organization Type
60004: Frequent Changes to Supplier Site	Supplier Model	Audit - Supplier Sites	• Address Name • Inactive Date • Payment Terms • Site • Status
60005: Frequent Changes to Supplier Payment Methods	Supplier Model	Audit - Supplier Payment Methods	• Default • Payment Method
60007: Changes to Supplier Bank Accounts on a Weekend	Supplier Model	Audit - Supplier Bank Accounts	• Account Name • Account Number • Bank Name
60018: Updates to Accounting Period Status	General Ledger	Audit - Accounting Period Status	• Accounting Period • End Date • Ledger • Period Number • Period Type • Start Date • Status • Year

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 20D
https://docs.oracle.com/en/cloud/saas/risk-management/20d/books.html

Key guides here include:

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

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

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.
Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.
Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120