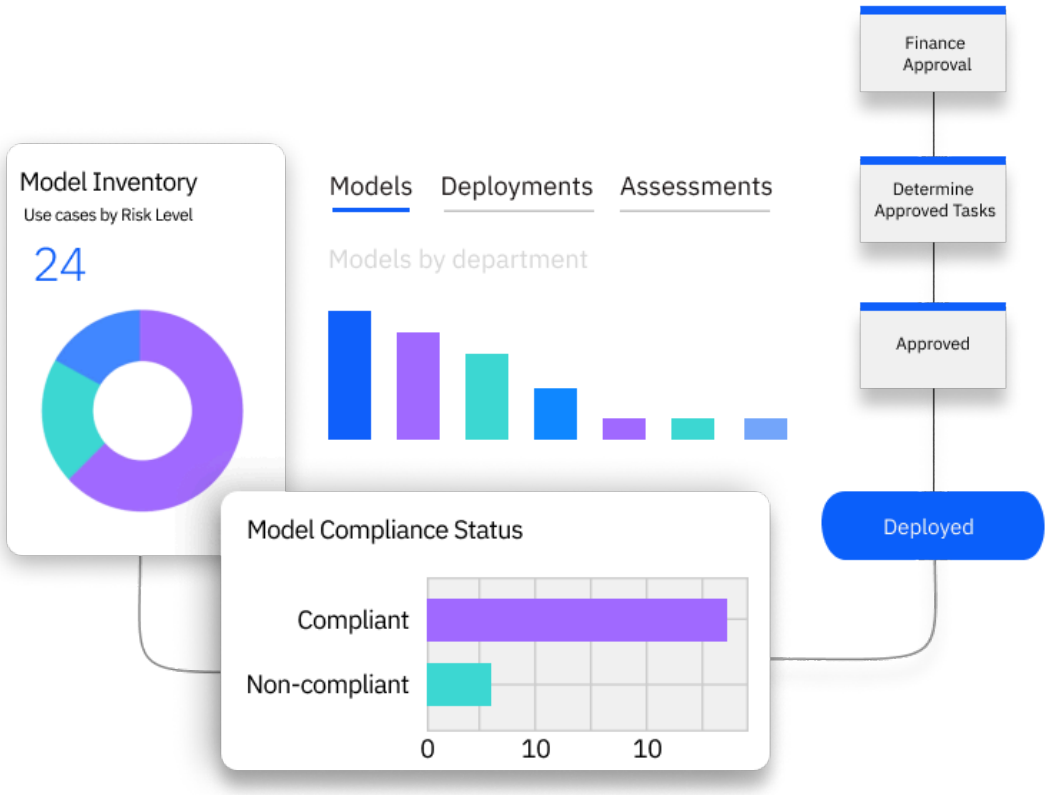
Monitor and Govern AI with watsonx.governance Day 2

Hands-on Lab Guide



Eric Martens
emartens@ibm.com

Contents

Day 2

Introduction

Welcome to part two of the Deloitte watsonx.governance hands-on lab. In this lab, you will explore the watsonx.governance solution from the perspective of an administrator, customizing the solution to fit a particular client.

In this lab, you will:

- Create business entities
- Customize object views
- Create questionnaires
- Modify existing approval workflows
- Configure model monitoring and metrics gathering
- Evaluate generative AI and machine learning models

A note on the environment

To complete this lab, you will use a Cloud Pak for Data software environment provisioned on IBM TechZone, with the watsonx.governance software installed. Your lab instructor will provide you with credentials to log into this environment.

Customization

It is important to understand that all the pieces of watsonx.governance that you will use in the following lab are fully configurable. AI use cases can be customized to include any level of detail the client requires. Workflows can be modified or built from scratch to reflect the client's approval processes. Relevant risks and the questionnaires that associate them with use cases can also be completely configured to meet a client's needs.

Troubleshooting

The environment you are using for this lab has been provisioned on IBM TechZone. Due to infrastructure constraints, you may experience some delay or slow performance. This frequently appears as error messages when saving changes to artefacts such as use cases or workflows. The vast majority of the time, the save was actually successful. Refreshing the screen will fix most of the issues; if this does not work, try the action again. If the action continues to fail, contact your lab instructor for more help.

Customize views

IBM OpenPages is an AI-driven, highly scalable governance, risk and compliance (GRC) solution that runs on any cloud with IBM Cloud Pak for Data. Its full capabilities are well beyond the scope of this lab. Instead, the lab will focus on the features that relate to governing models: customizable workflows and alerts, integration with Factsheets, and the ability to get an enterprise-wide view of the status of AI and machine

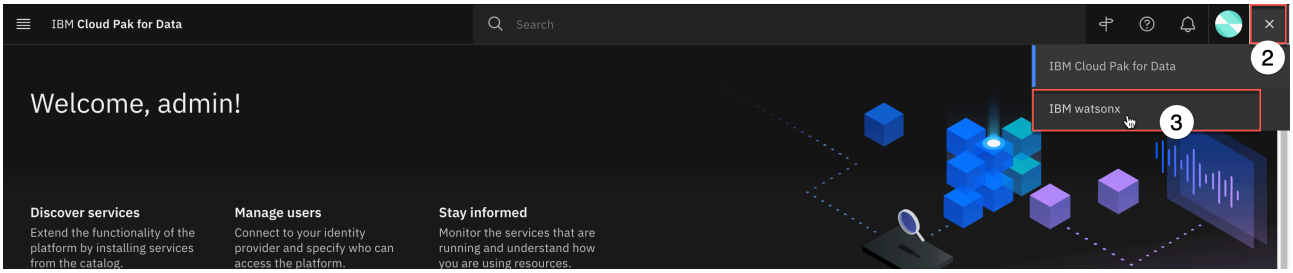
learning initiatives. In the context of watsonx.governance, the OpenPages solution is referred to as the governance console. However, in many locations in the user interface, you will see it being referred to as OpenPages.

The watsonx governance console can be fully customized to fit an individual organization. Your lab instructors have loaded sample user and organization data to more fully flesh out the business. For the first several sections of the lab, you will customize business entities and modify views and workflows to see how the solution can be customized to meet an organization's requirements. These customizations would be performed by an administrator persona, responsible for configuring the watsonx.governance solution for the organization.

1. Switch contexts

The IBM watsonx context offers an improved user interface and better integration for AI governance than the Cloud Pak for Data context, and offers expanded functionality such as monitoring for detached prompt templates. Some operations, such as creating a database, currently require using the Cloud Pak for Data context. However, for the remainder of the lab, you will use the IBM watsonx context.

1. Log into the Cloud Pak for Data home page using the credentials from your reservation.
2. Click on the grid icon in the upper right to open the context menu.
3. Click on the IBM watsonx menu item to change the context. A Welcome to watsonx popup window may open.



4. Close the popup window, or click the Take a tour button if you wish.

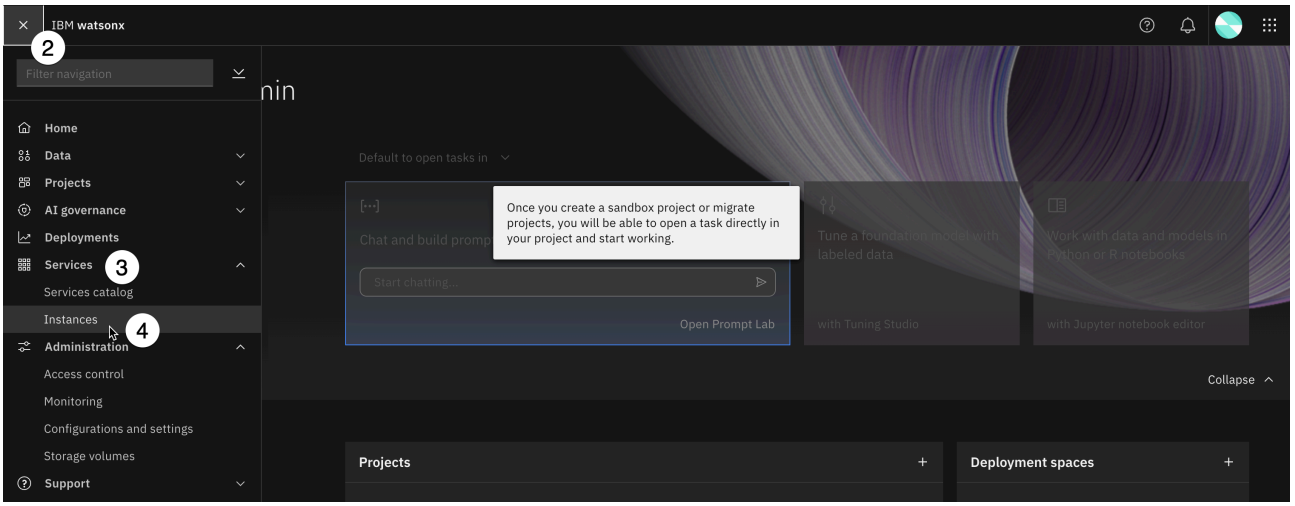
Your screen should now show IBM watsonx branding. This screen will be referred to throughout the lab as the watsonx home screen.

> Note: You will likely need to switch to the watsonx context every time you sign in to your environment.

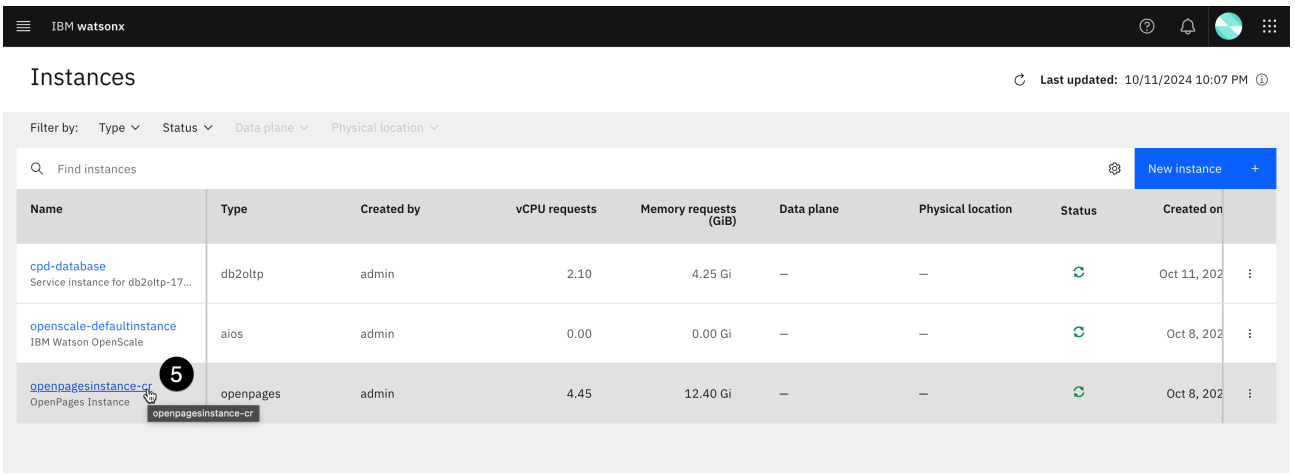
2. Launch the governance console

In this section, you will launch the OpenPages service.

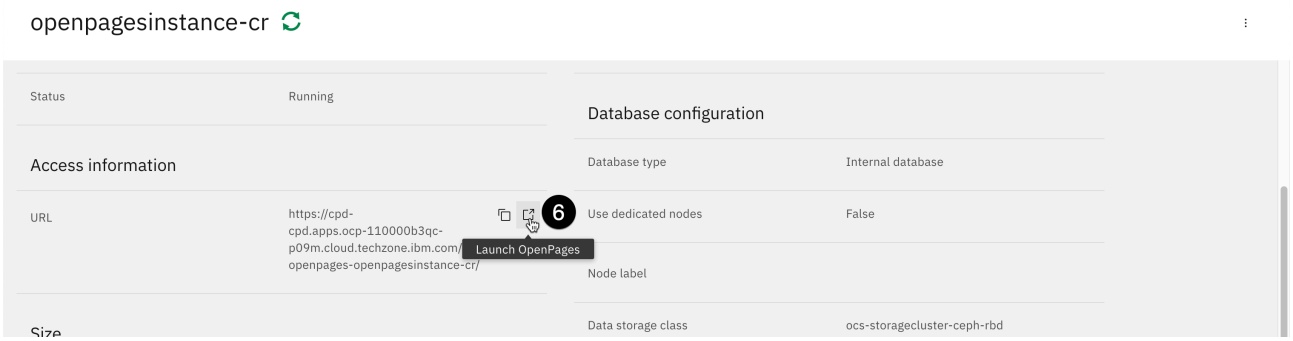
1. If necessary, return to the watsonx home page by clicking the IBM watsonx link in the upper left.
2. Click on the hamburger menu in the upper left.
3. Click on the Services item from the menu to expand it.
4. Click on Instances to open the Instances screen.



5. Locate the instance of OpenPages in the table and click on the link in the Name column to open the instance details screen.



6. Scroll down to the Access information section, and click the launch icon to launch the service.



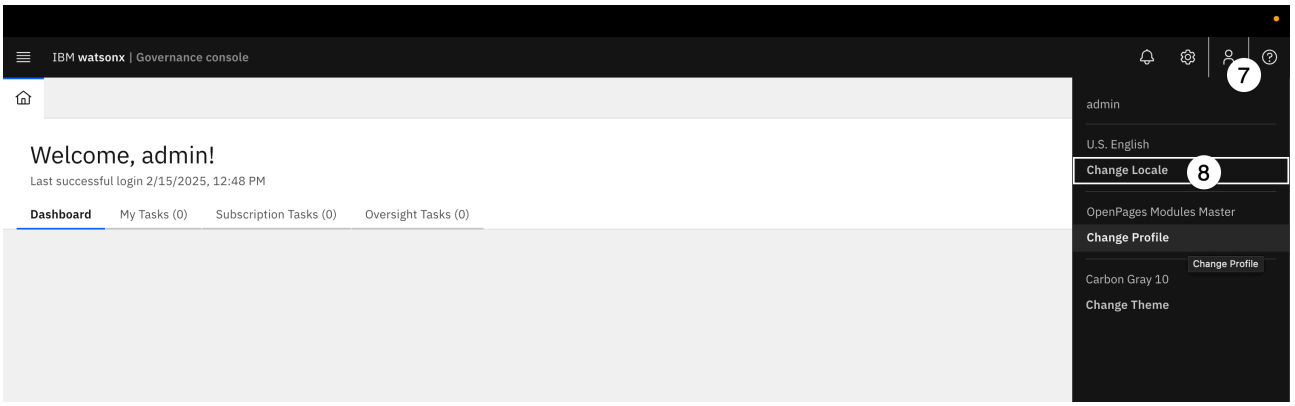
The OpenPages service launches in a new browser tab.

The governance console determines what a user sees based on that user's current profile. Users can have multiple profiles assigned to them, and can switch between them based on what task they are trying to accomplish. Like all things in the governance console, administrators can customize the views that each profile sees, or even create new profiles with entirely bespoke views.

For the rest of this lab, you will use the *watsonx-governance MRG Master* profile, which will allow you to view all information related to model risk governance (MRG).

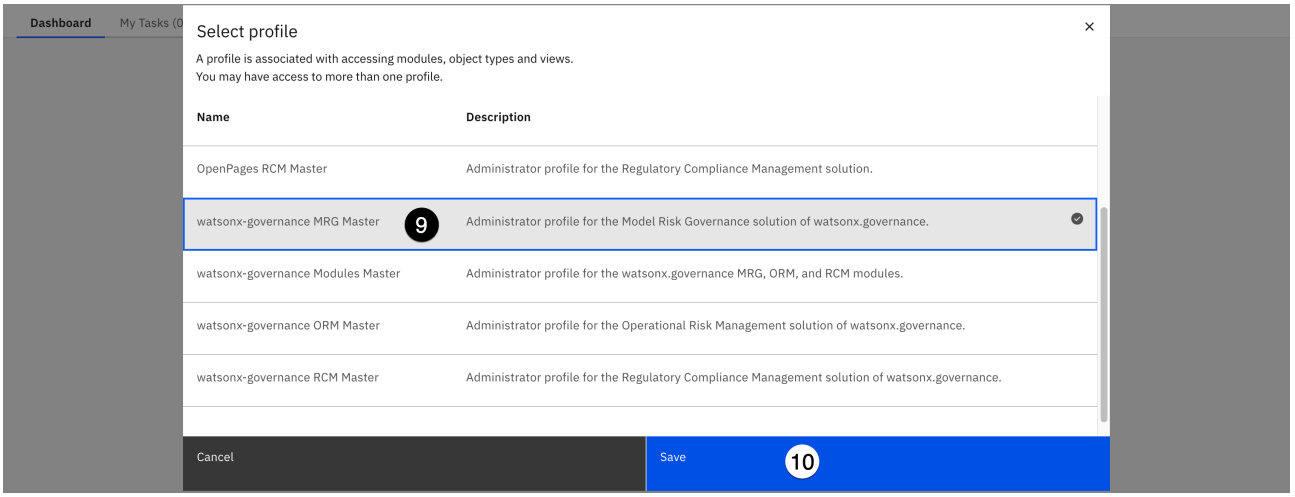
7. Click on the avatar icon in the upper left to open the user menu.

8. Click on the Change Profile menu item. The Select profile dialog box opens.



9. Click on the watsonx-governance MRG Master profile from the list to select it.

10. Click on the Save button to save your selection.



Your home screen should change, showing a variety of graphs on your dashboard.

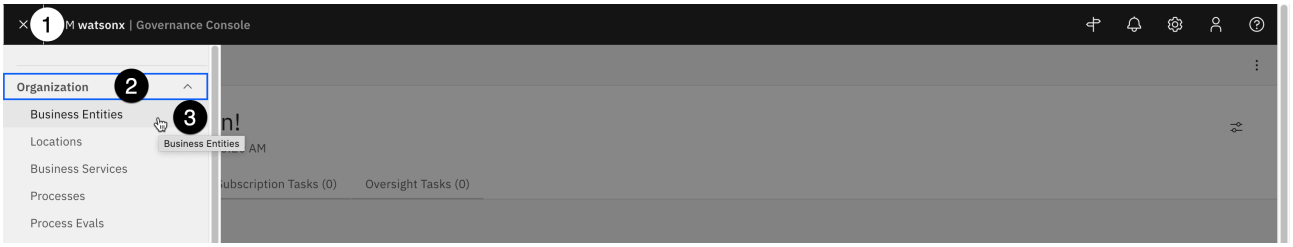
3. Create a business entity

Next, you will create a business entity, which is an abstract representation of a business structure. During the setup for this lab, your lab instructor loaded a FastMap file into the governance console. That file contained the structure for the High Oaks bank organization, including a Human Resources department. In the steps below, you will create a *Regulatory Compliance* entity beneath the *Human Resources* organization.

1. From the watsonx governance console home screen, click the hamburger menu in the upper left.

2. Click the Organization menu item to expand it.

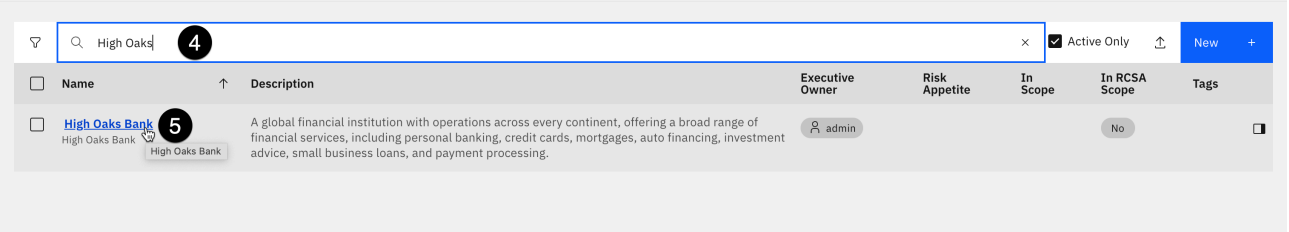
3. Click on Business Entities. The Business Entities tab opens.



4. Type High Oaks in the Search field and press the Return key to narrow the list of business entities.

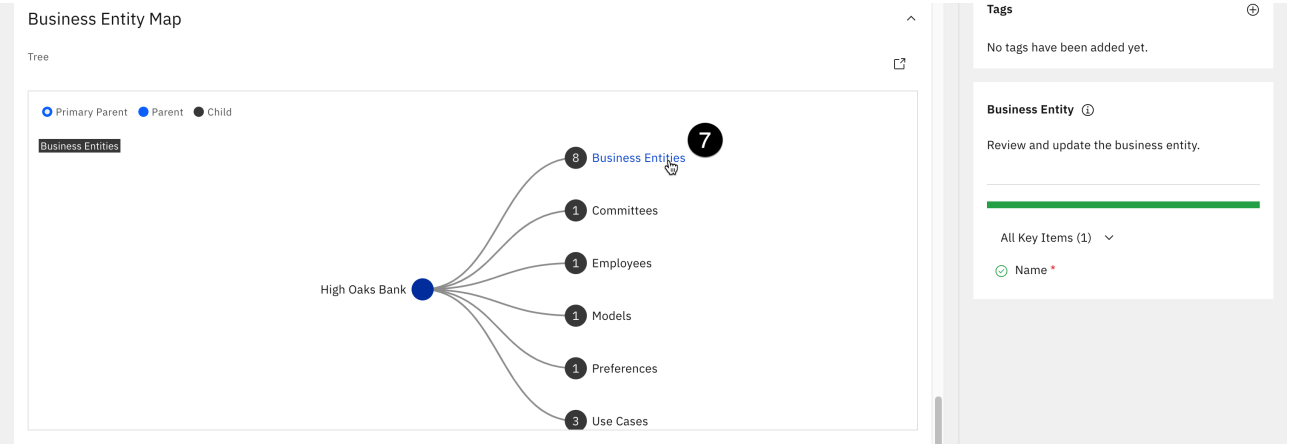
5. Click on the link for High Oaks Bank in the table to open the entity.

Business Entities (1)



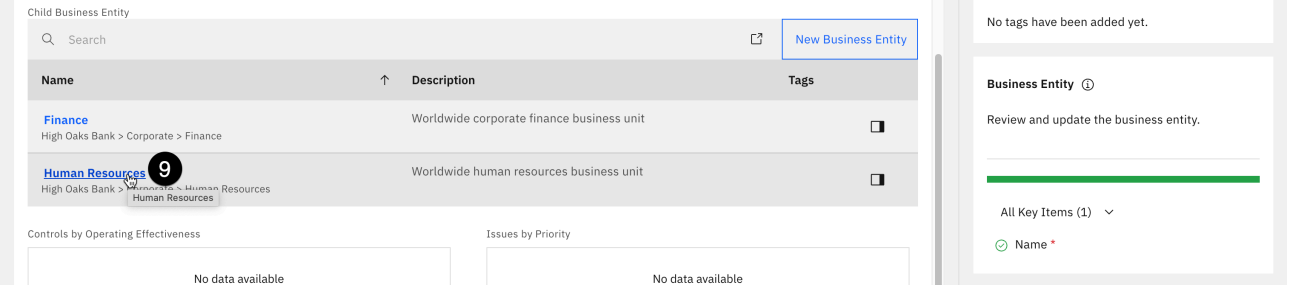
6. Scroll down to the Business Entity Map section of the page, which shows a tree view of the different entities beneath the High Oaks bank entity. Note that the High Oaks Bank parent entity contains a variety of children, including other business entities, employees, models, and use cases. This view is a convenient way to quickly see all the different items associated with a part of an organization.

7. Click on the Business Entities item in the tree view. The Children of High Oaks Bank view opens in a new pane on the right of the screen.



8. Each of the child entities is represented by a tile in the view. Scroll down to the Corporate entity tile and click on it. A new tab opens to display the information for the Corporate business entity.

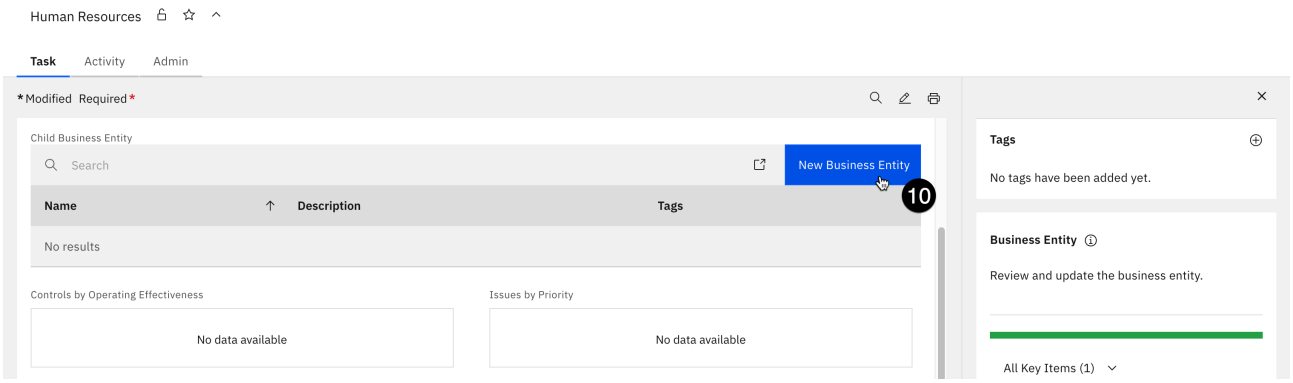
9. Scroll down to the Child Business Entity table in the General section of the screen and click on Human Resources to open a new tab for that entity.



Note that the Human Resources entity does not have any child business entities. If you scroll down to the Business Entity Map, you will see that it does contain models and use cases that are unique to this business

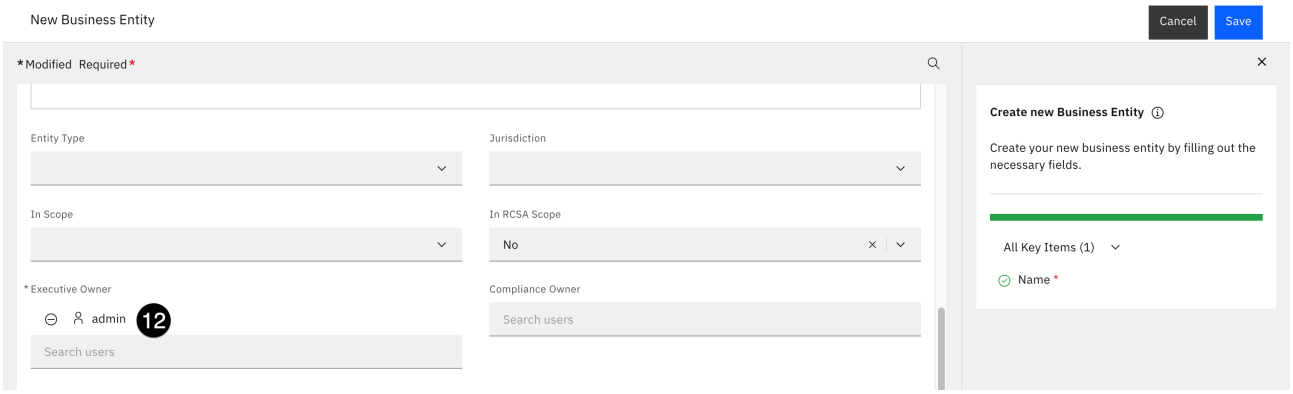
entity. These sample models and use cases were loaded during the environment configuration step, when you loaded the Fastmap spreadsheet file.

10. Scroll back to the Child Business Entity table and click the New Business Entity button.



11. Enter Regulatory Compliance in the Name field.

12. Enter admin in the Executive Owner field.



Note that the Primary Business Entity has been pre-populated with the Human Resources entity, though you can change it if you wish. Also note that the Create new Business Entity progress bar on the right shows that the one required field has been completed, turning the status bar green and enabling the Save button.

13. Click Save to save the business entity.

The *Regulatory Compliance* business entity has been created in the governance console, and will appear as a child of the Human Resources entity.

When customizing the governance console for clients, you can create business entities manually in this fashion. You can also create formatted spreadsheets, which can be uploaded to create the entire organizational structure more quickly. Creation of these FastMap spreadsheets is beyond the scope of this lab.

4. Create a custom field for the use case view

Watsonx.governance uses the concept of model use cases to organize machine learning and AI solutions to business problems. A model use case represents a single problem an organization is attempting to address

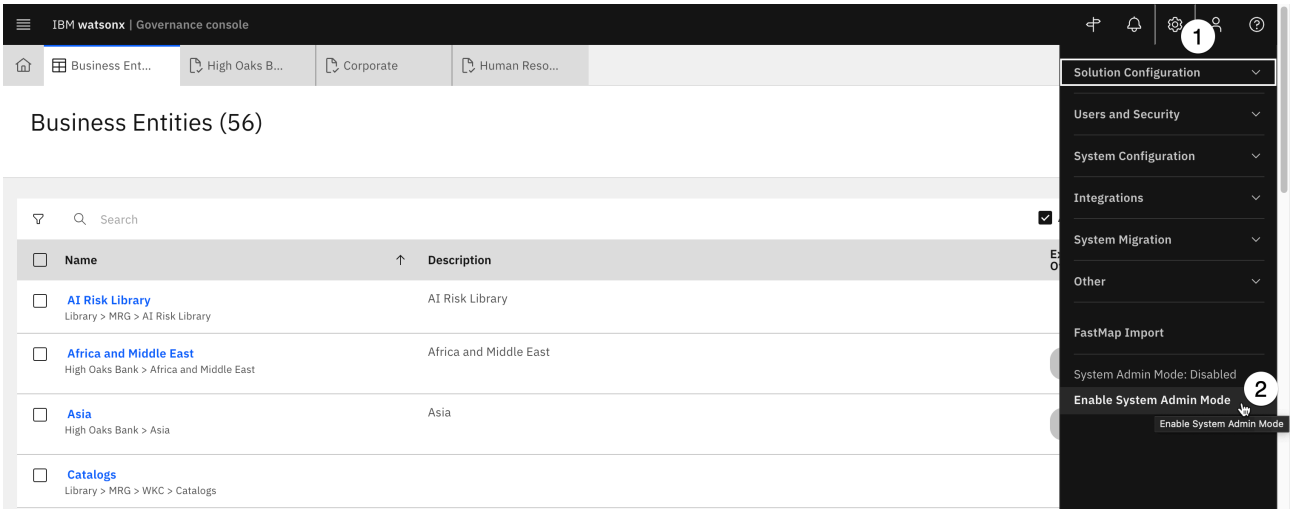
with AI or machine learning. Many different models can be associated with a use case, whether they are in development, testing, or production phases.

There are no defined global standards for information that must be included in a use case; while there is a minimum set of information such as model metadata and performance metrics that should be present, specifics will vary widely between different industries and different organizations. The watsonx governance console is fully customizable to allow clients to tailor the forms and processes to their exact needs.

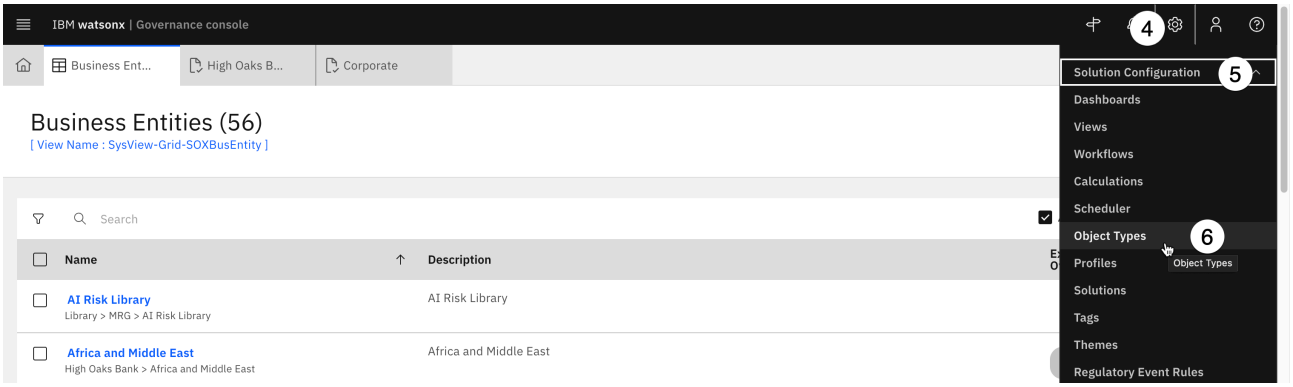
In this step, you will add a new field to the use case view. This particular example adds the Secondary EU AI Review field; however, when performing the exercise, think about clients you have worked with in the past and any specific requirements for information gathering that they presented.

To add a field to the internal database, you must first enable changes to the system.

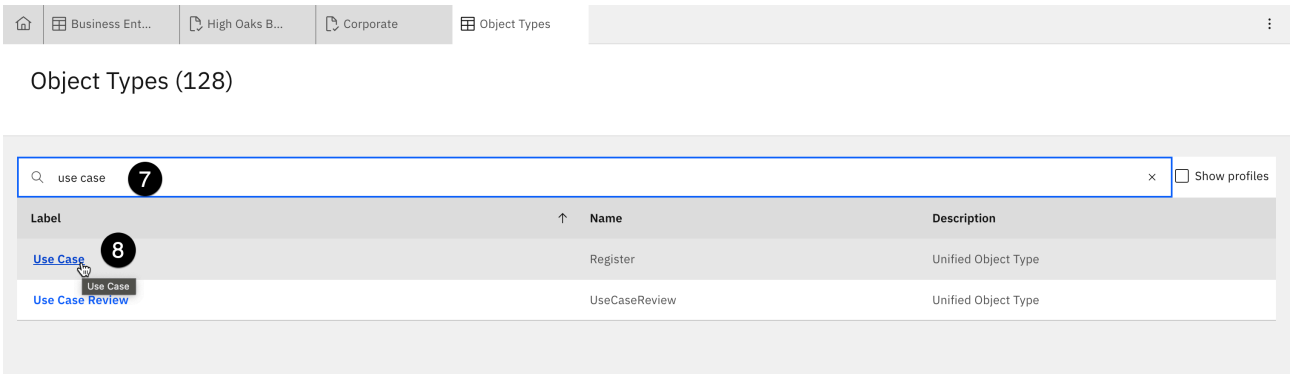
1. Click the gear icon in the upper right to open the Administration menu.
2. Click Enable System Admin Mode to enable changes.



3. A popup window will open, prompting you to confirm your choice, and notifying you that while the mode is enabled, the system will be unavailable to other users. Click the Enable button to confirm.
4. Click on the gear icon again to open the Administration menu.
5. Click on the Solution Configuration menu item to expand it.
6. Click on the Object Types menu item. The Object Types tab opens.

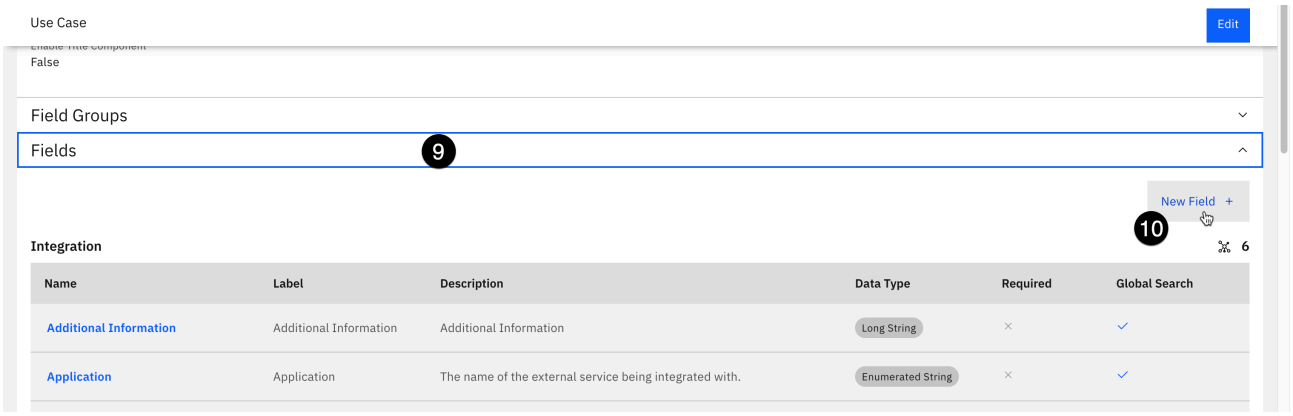


7. Enter use case in the search field to narrow the list of object types.
8. Locate and click on Use Case from the table to open the Use Case object.

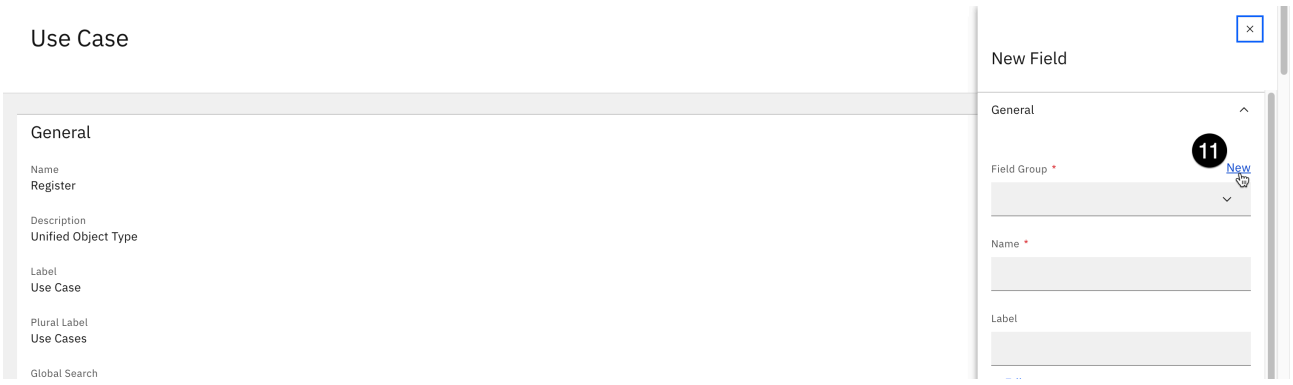


9. Click on the Fields section to expand it. All the fields currently associated with model use cases are listed in their existing groups.

10. Click on New Field to open the New Field panel.



11. You will place the field in a new grouping. Click the New button above the Field Group dropdown. The New Field Group panel opens.

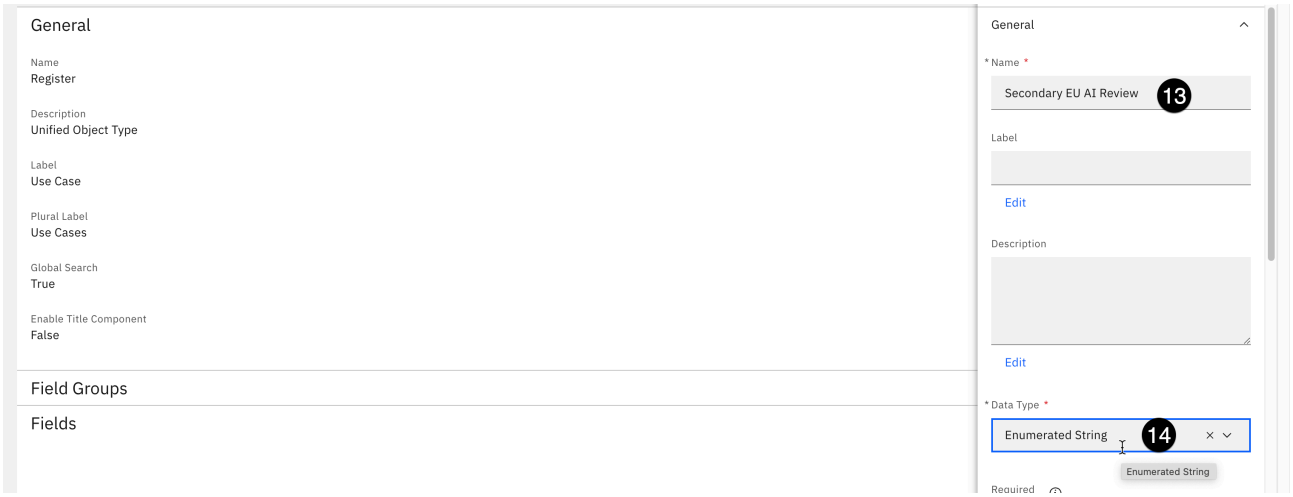


12. Enter EU Compliance in the Name field and click the Create button to create the grouping. The New Field panel updates, showing that the field is now contained in the EU Compliance group. Note that there is already a Compliance field group in the use case, and, strictly speaking, the field you are creating could go there. In this lab you are creating a new group to see how it could be done for other fields the client may want to create.

> Note: If network conditions are slow, or if computing resources in the environment are limited, you may receive an error message when saving the new field group. The vast majority of the time, the field group has actually been saved. Refreshing the page, creating a new field, and selecting the EU Compliance group from the Field Group dropdown will fix the issue.

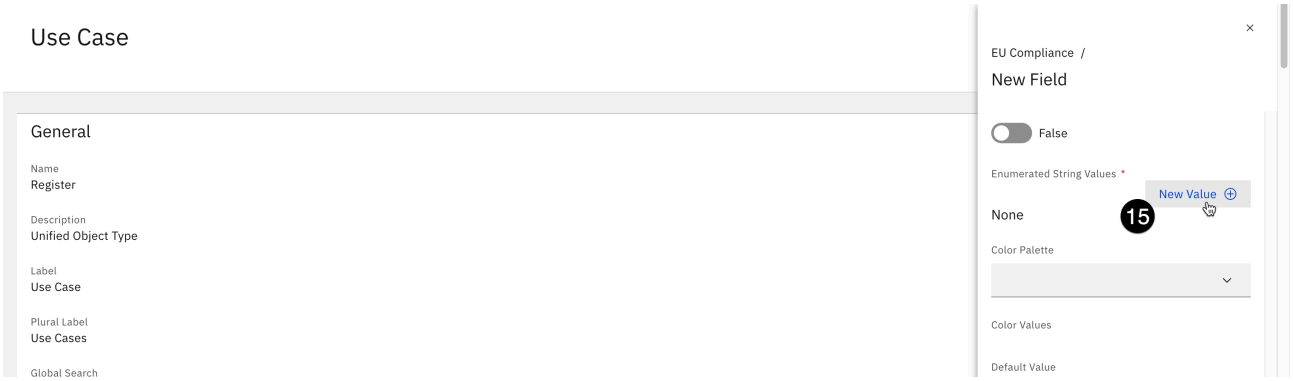
13. Enter Secondary EU AI Review in the Name field.

14. Click the Data Type dropdown and select Enumerated String. This data type will appear as a dropdown in the form. Note the other data types, including strings, integers, booleans (true/false), dates, currencies, and more.



Note that you have the option to set the field to Required using the toggle. However, DO NOT set the field to required at this time, as it will prevent approval actions from being taken. You can also set default values and descriptions.

15. Scroll to the Enumerated String Values section and click the New Value button. The New Enum Value panel opens.



16. Enter Approved into both the Name and Label fields and click Create.

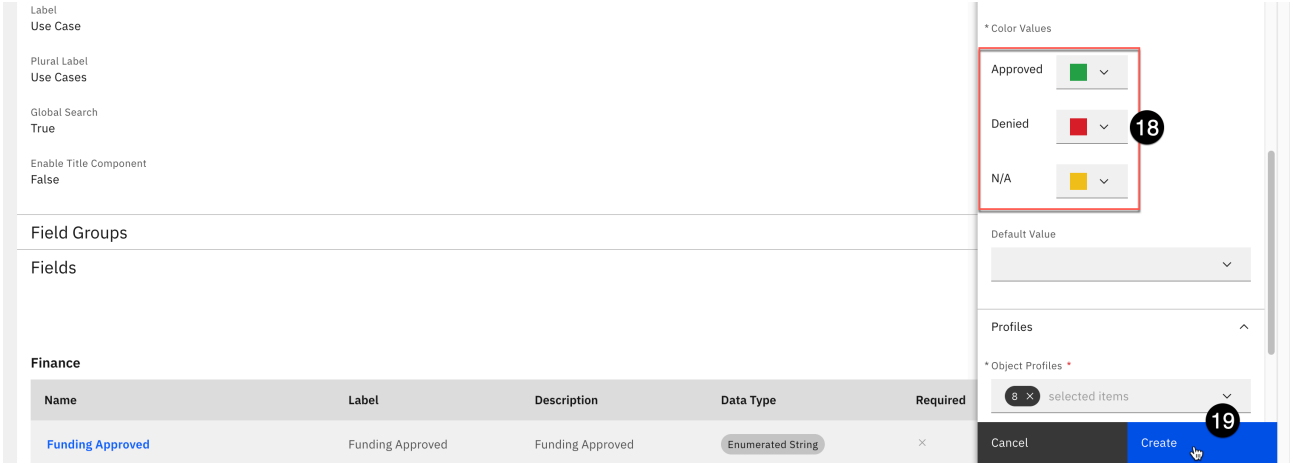
17. Repeat steps 15 and 16 to add Denied and N/A values.

Note that you can set colors for the different values, which will show on the icon badges when the form is completed.

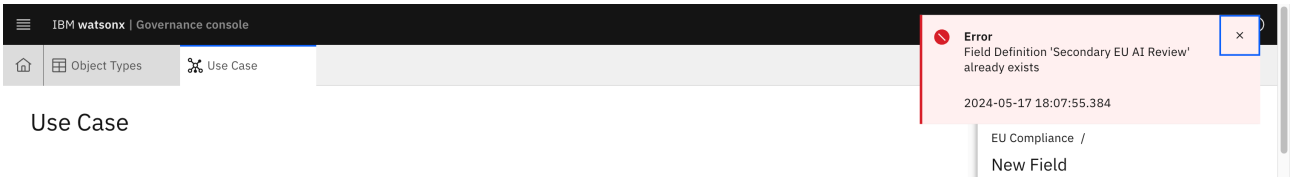
18. Assign colors to the values using the dropdowns.

Note that you can also select which object profiles (such as the watsonx profiles you assigned to users in previous steps) are allowed to interact with the field

19. Click Create to add the new field to the object.



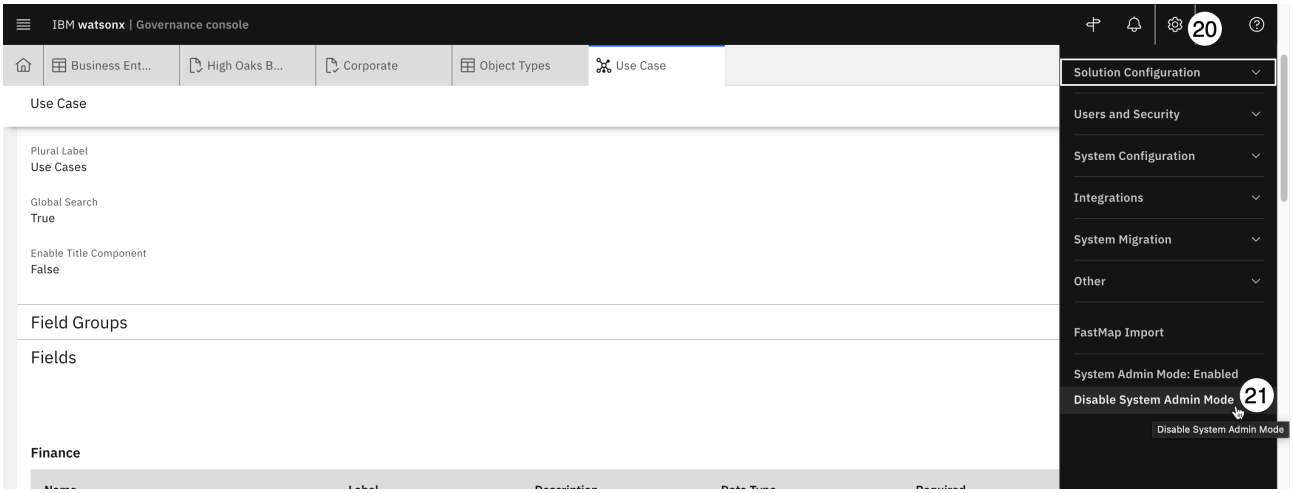
Note that, occasionally, saving the field can take longer than expected and results in a Network error or the error message below:



If you get this message, try and save the field again. If you receive an error that the field already exists, then most likely the changes were saved successfully. Close the New Field panel and refresh the page, and you should see the field listed in the Fields section.

To allow other users to access the governance console again, you will need to disable system admin mode.

20. Click on the gear icon to open the Administration menu.
21. Click on Disable System Admin Mode to return the console to its normal state.



Once again, you will be prompted to confirm your choice. Click Disable to confirm.

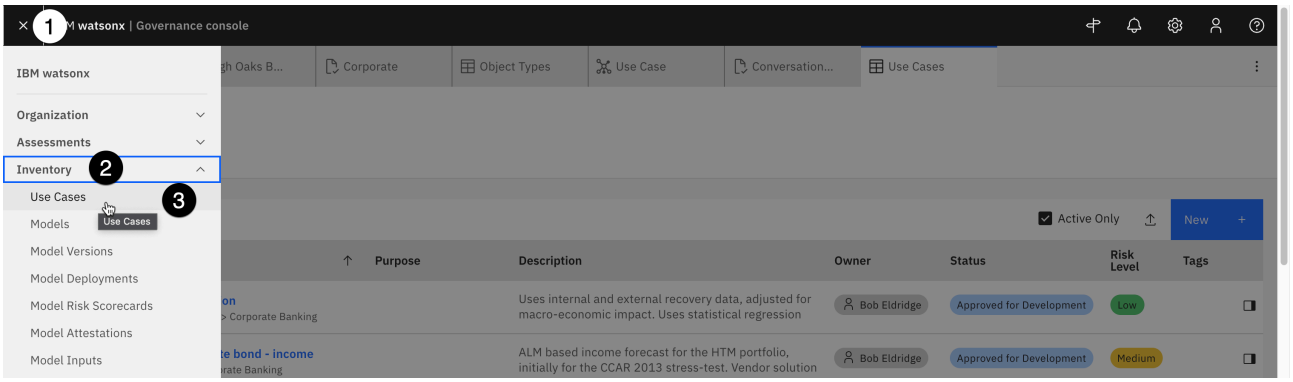
5. Add the custom field to the use case view

In the previous section, you created a custom field. In this section, you will add that field to the view for use cases so that it can be included. Note that the system views cannot be modified; instead, you will copy the existing view, make changes to the copy, and then set your modified view as the new default.

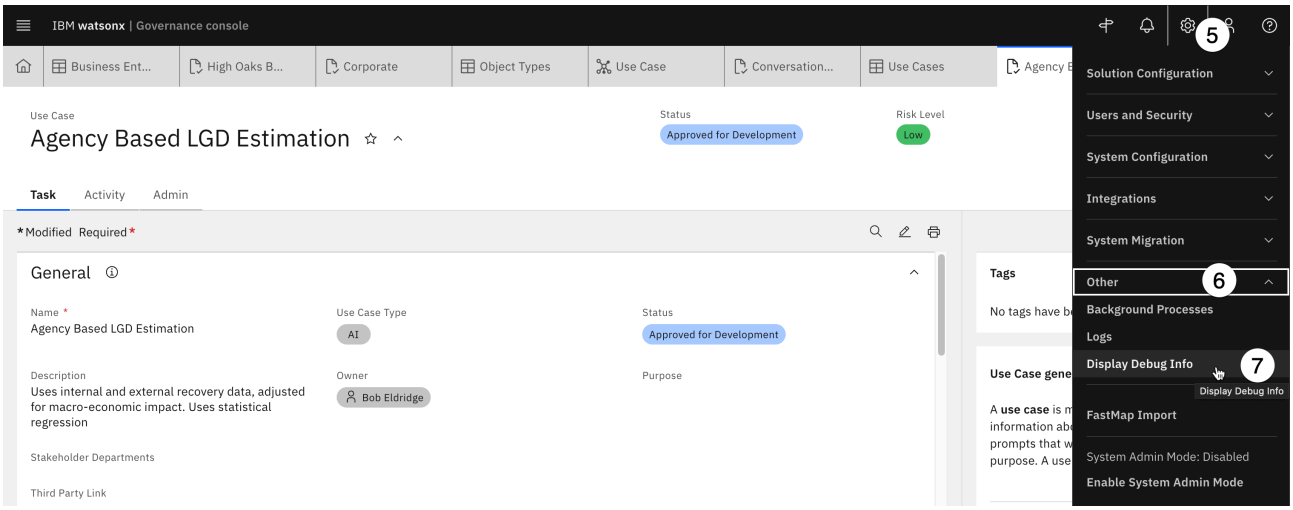
To create a copy of a system view, you could locate the view from the inventory. However, there are hundreds of views included in the console, and it is not always clear which view corresponds with the object

you wish to edit. Fortunately, there is a shortcut built into the system to identify which view is being shown.

1. Click on the hamburger menu in the upper left.
2. Click on the Inventory menu item to expand it.
3. Click on the Use Cases menu item. A new tab opens listing all existing use cases.



4. Click on any use case from the list to open it.
5. Click on the gear icon in the upper right to open the Administration menu.
6. Click on the Other menu item to expand it.
7. Click on the Display Debug Info menu item.

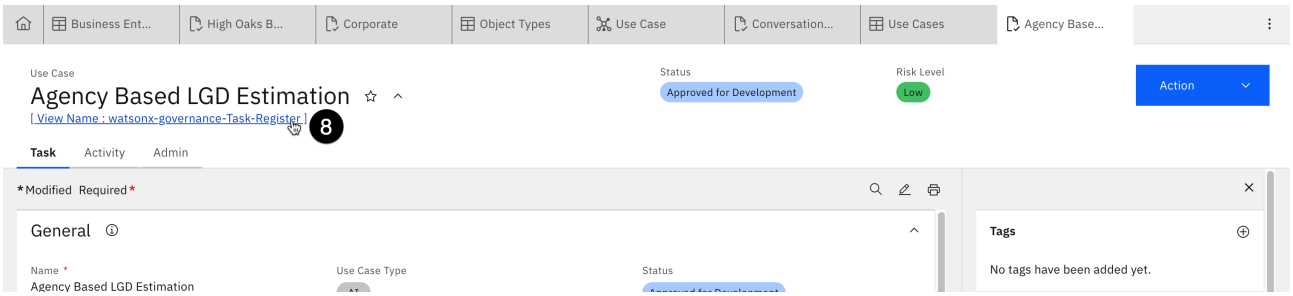


A link will appear beneath the name of the use case, identifying the view as watsonx-governance-Task-Register.

> Note: If the default view name shows as SysView-Task-Register, then the admin user is not using the correct profile. Follow instructions on changing your profile from the 2. Launch the governance console section above to ensure that the watsonx profiles are assigned, and that the admin user has changed to one of those profiles.

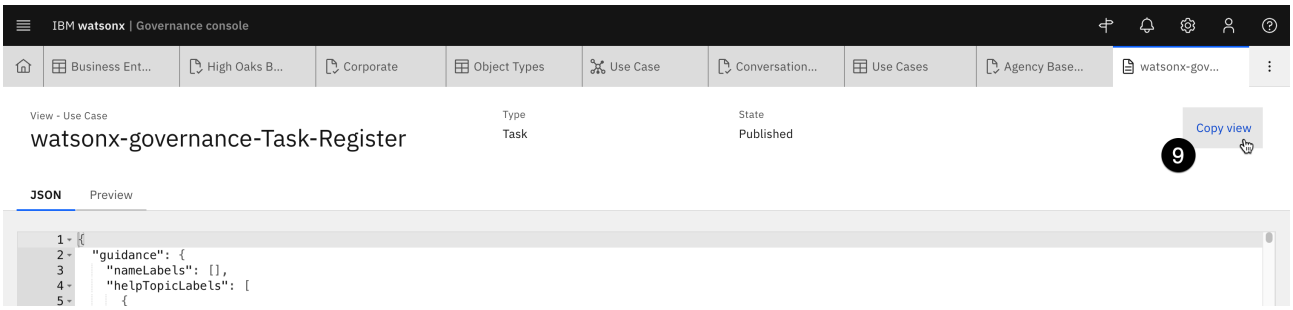
The *Display Debug Info* option is extremely useful for determining the view that is showing on a given screen, making it easier to find and customize that view.

8. Click the link for watsonx-governance-Task-Register to open the view in a new tab.

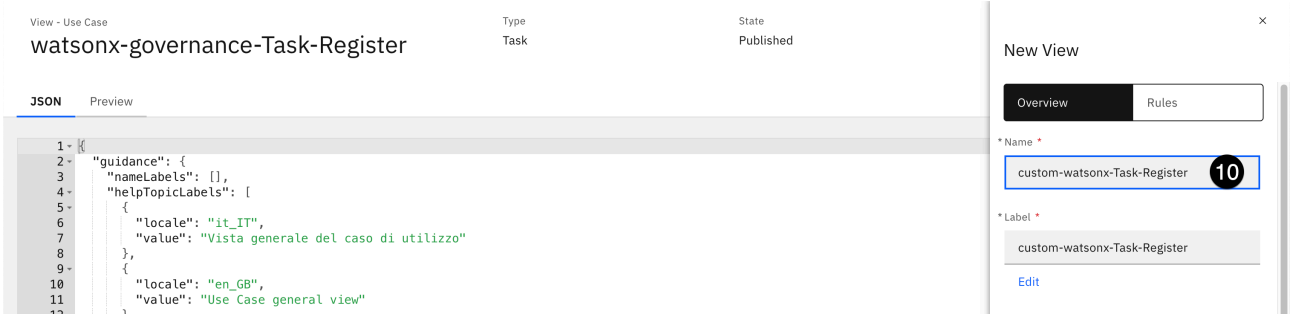


A warning message appears in the top right of the new tab, informing you that this is a read-only system view and cannot be changed.

9. Click the Copy view button just below the warning message. The New View panel opens.

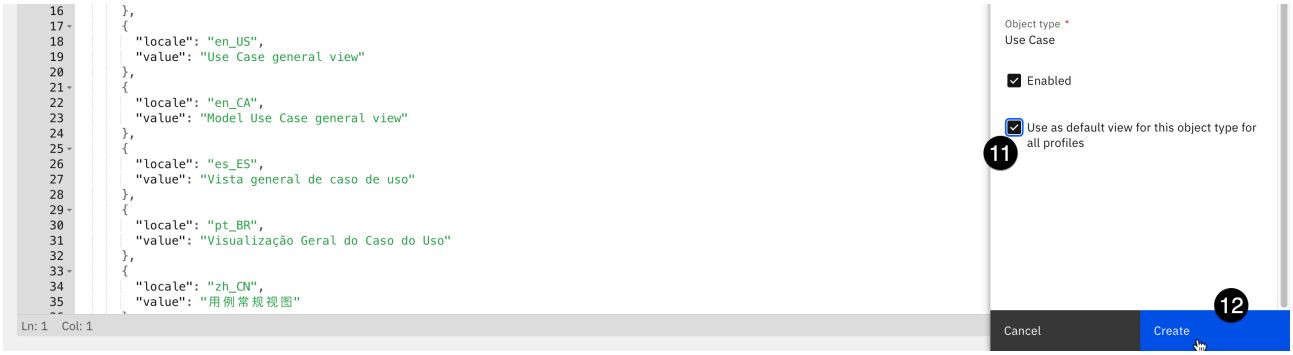


10. Enter a name for your view in the Name field. Staying consistent with the watsonx views will make it easier to locate later, so choose a name like custom-watsonx-Task-Register. Your text entry will be automatically mirrored in the Label field.



11. Scroll to the bottom of the New View panel and check the box next to Use as default view for this object type for all profiles.

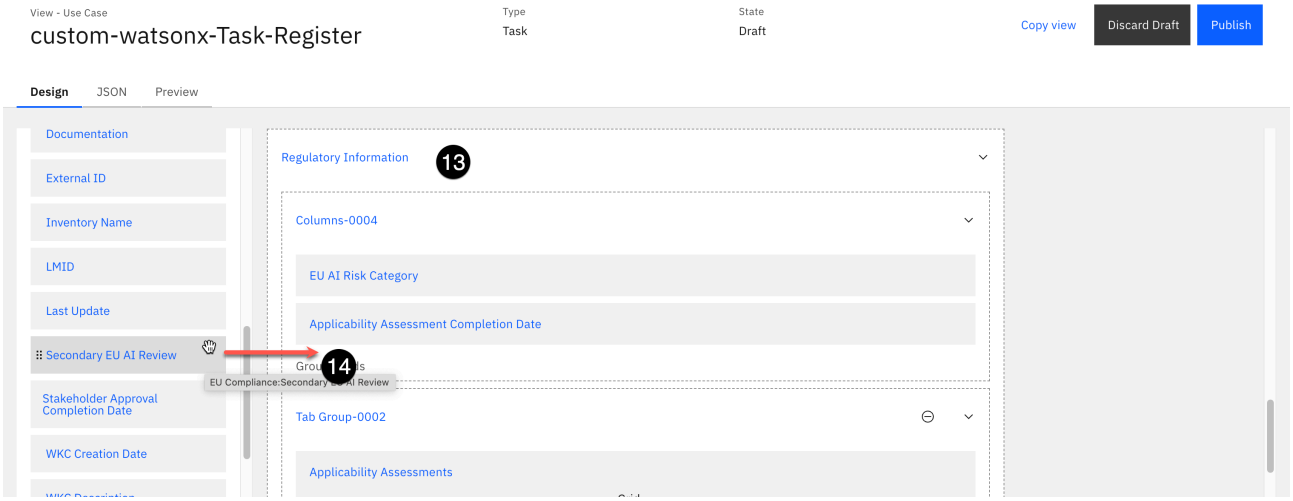
12. Click Create to create the view.



When the view has finished saving, note that there is now a Design tab that allows you to change the design of the form in the view. Available fields that are not already included in the view are located in the left panel. The center panel shows the current layout of the view, divided into sections such as Header, General, and Use Case Details.

From this view, you can create new sections of the form by scrolling to the bottom of the screen and clicking the New section button. However, since the field you will be adding is related to government regulations, you will use the existing Regulatory Information section.

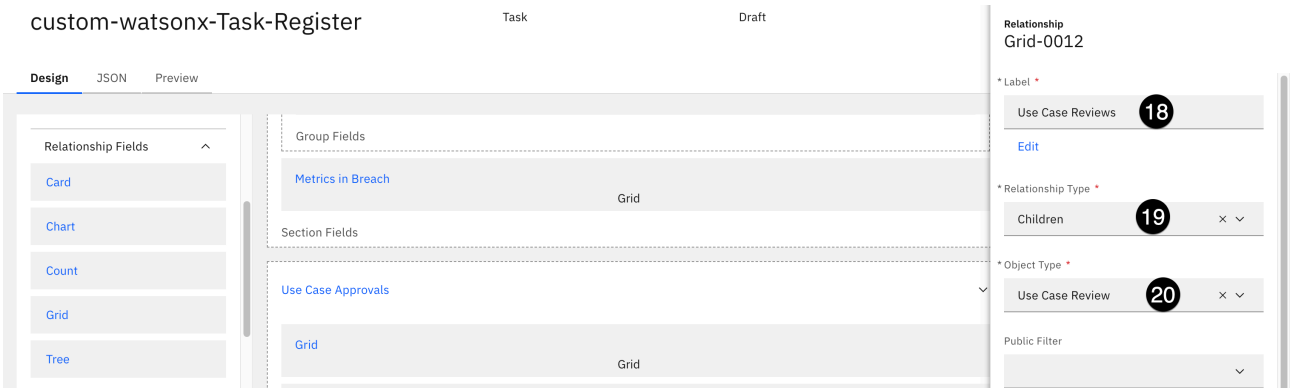
13. Scroll to the Regulatory Information section of the center panel.
14. Scroll to the Object Fields section of the left panel. Click and drag the Secondary EU AI Act Review object into the Regulatory Information section in the center panel beneath the Applicability Assessment Completion Date item.



Next, you will need to add the Use Case Review fields to the view.

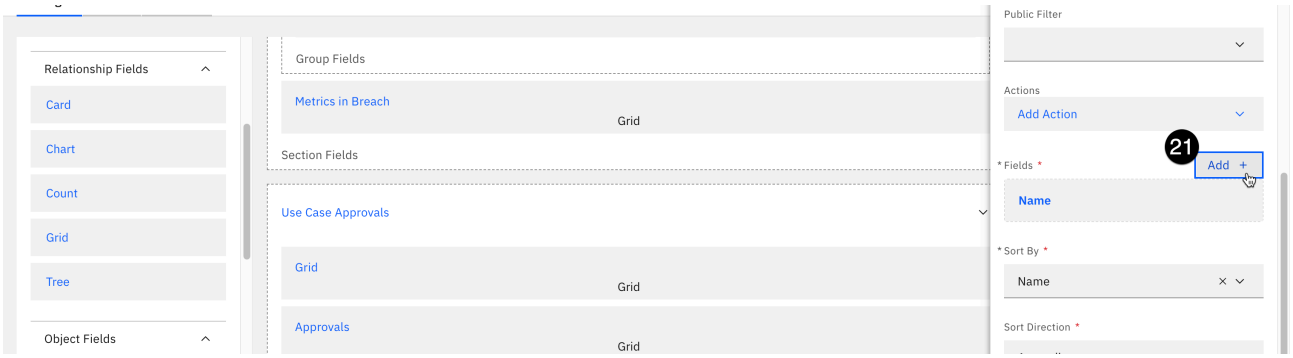
15. Scroll the main window to the Use Case Details section.
16. Scroll the left panel to the Relationship Fields section.
17. Click and drag the Grid item from the left panel into the Use Case Details section. The Relationship panel opens on the right side of the screen.

18. Enter Use Case Reviews in the Label field.
19. Click on the Relationship Type dropdown and select Children.
20. Click on the Object Type dropdown and select Use Case Review.



The pending use case reviews will now show in this section of the view; however, it would be even more helpful to show their status, and the department responsible for reviewing them.

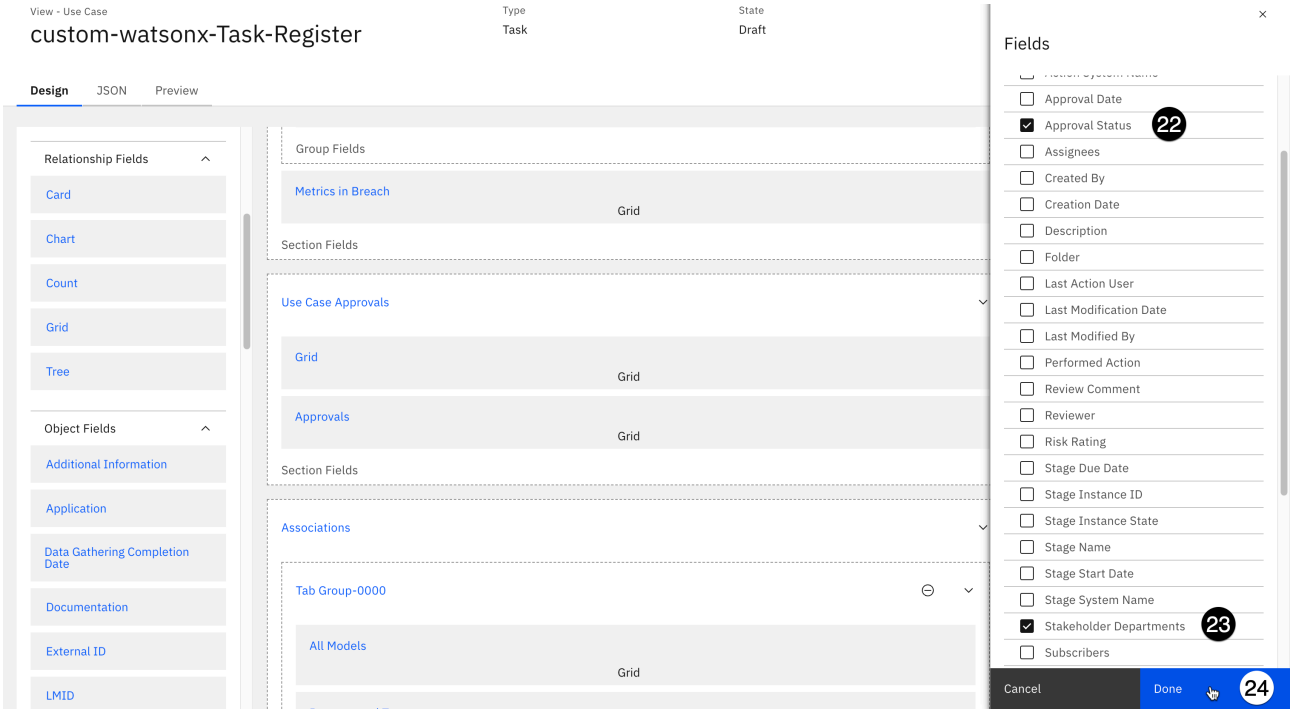
21. Scroll down to the Fields section and click the Add button. The Fields panel opens, showing all of the available fields for use case reviews.



22. From the list of fields, check the box to the left of the Approval Status item.

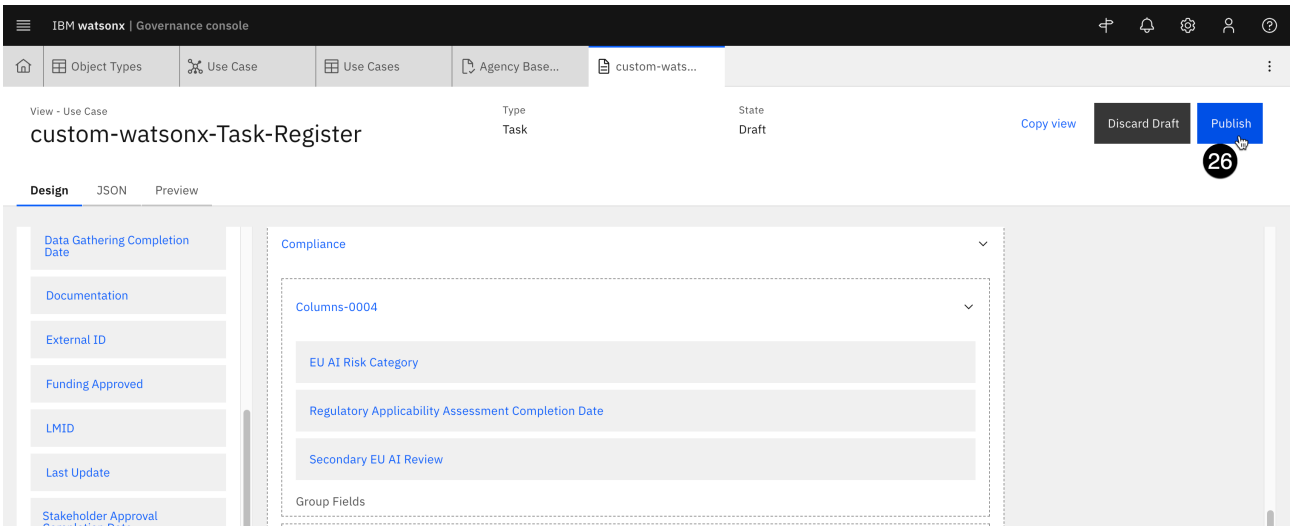
23. From the list of fields, check the box to the left of the Stakeholder Departments item.

24. Click the Done button to add the new fields to the grid. The Fields panel closes.



25. Click the Done button to finalize your changes to the grid and close the Relationship panel.

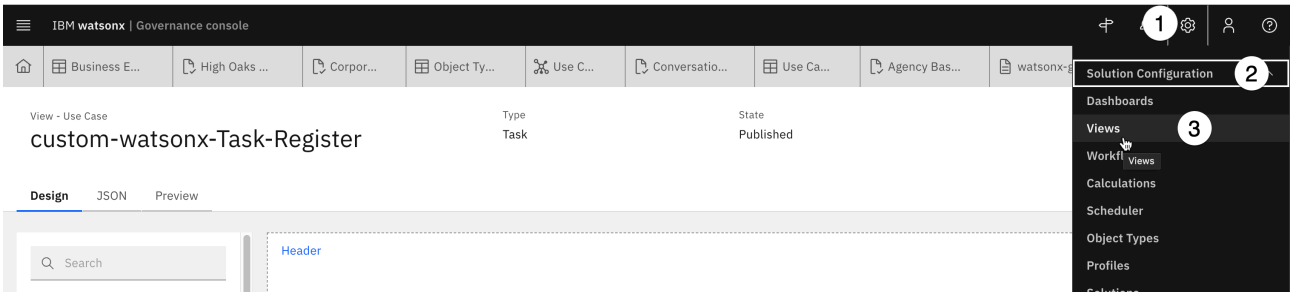
26. Click Publish in the upper right to publish your changes to the view.



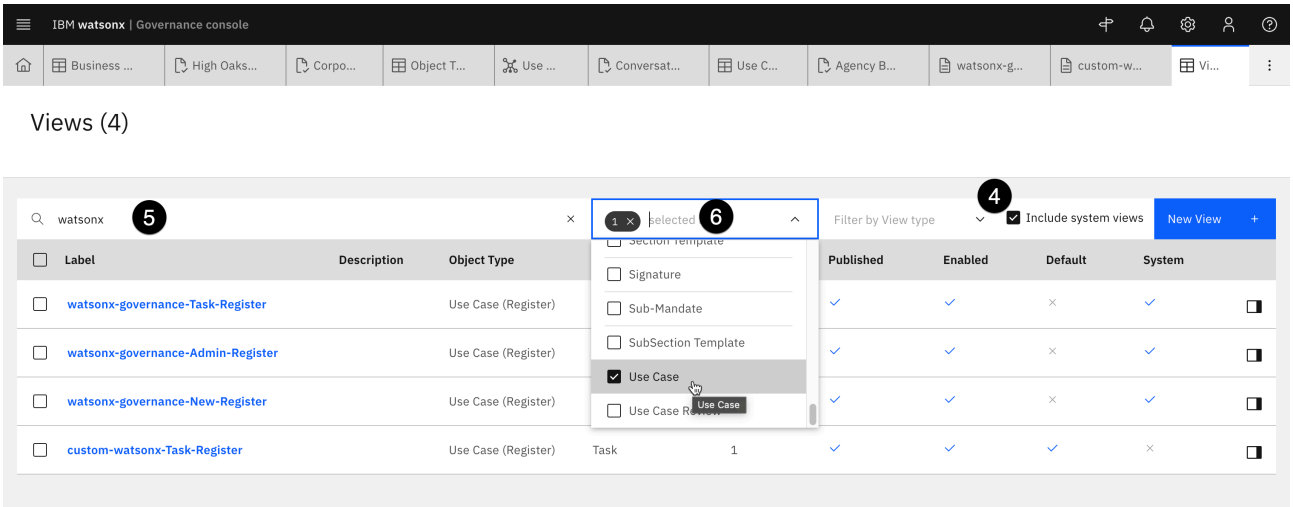
6. Disable the old view

You have successfully updated the use case view to include your new custom field. However, the new view may not show for all model use cases. In this section, you will disable the default system view, which will cause your changes to appear for all use cases.

1. Click on the gear icon to open the Administration menu.
2. Click on the Solution Configuration menu item.
3. Click on the Views menu item to open a new tab listing all the views.



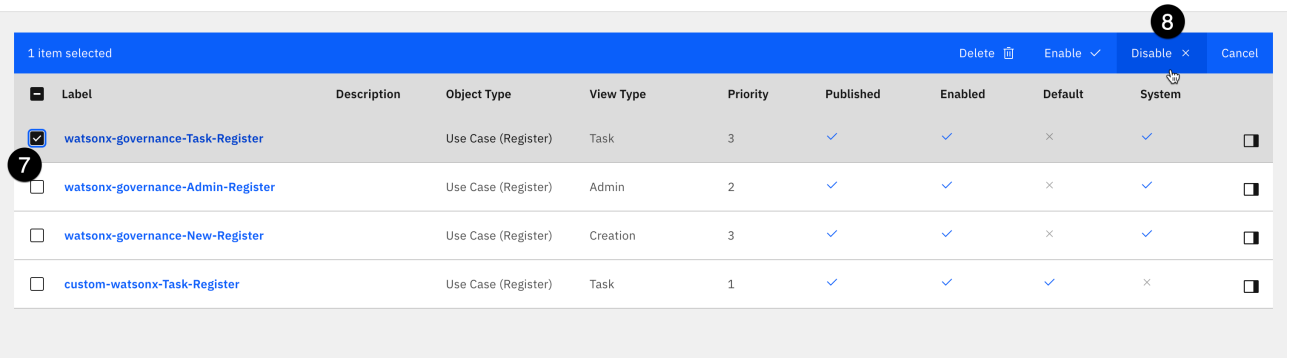
4. Ensure that the Include system views box is checked.
5. Enter watsonx in the search field to narrow down the results.
6. Click on the Filter by Object type dropdown and select Use Case to further narrow the search results.



7. Click the box next to the watsonx-governance-Task-Register system view.

8. Click Disable from the context menu above the table.

Views (4)



You have successfully disabled the system view, ensuring that the new view with the custom field (*custom-watsonx-Task-Register*) will now appear for all use cases as long as the user has the watsonx profiles enabled for their account. You can open an existing use case to see the new field if you wish.

Create a questionnaire template and custom workflow

The watsonx governance console provides the ability to create and employ questionnaires to assist in the governance process. As with all elements of the governance console, questionnaires are fully customizable, and can be configured to automatically trigger further actions such as use case reviews, audits, communications, alerts, and more.

In this section of the lab, you will see how the questionnaire editor works by creating a form to edit the custom field you created in the previous step, allowing the compliance officer to fill out a form for their secondary review.

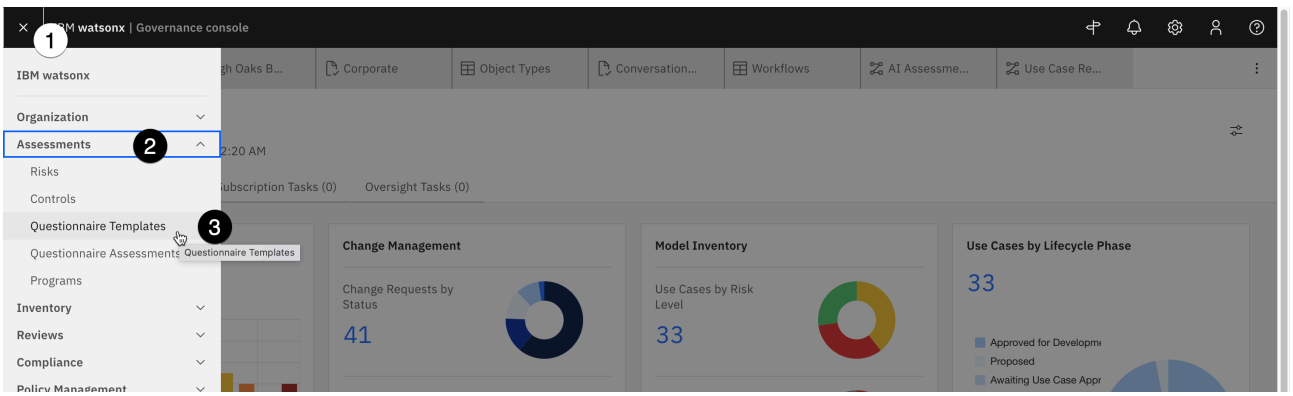
Finally, you will add the questionnaire as a part of the built-in AI assessment workflow, which will then allow you to integrate the questionnaire into the workflow for approving model use cases.

1. Create the questionnaire template

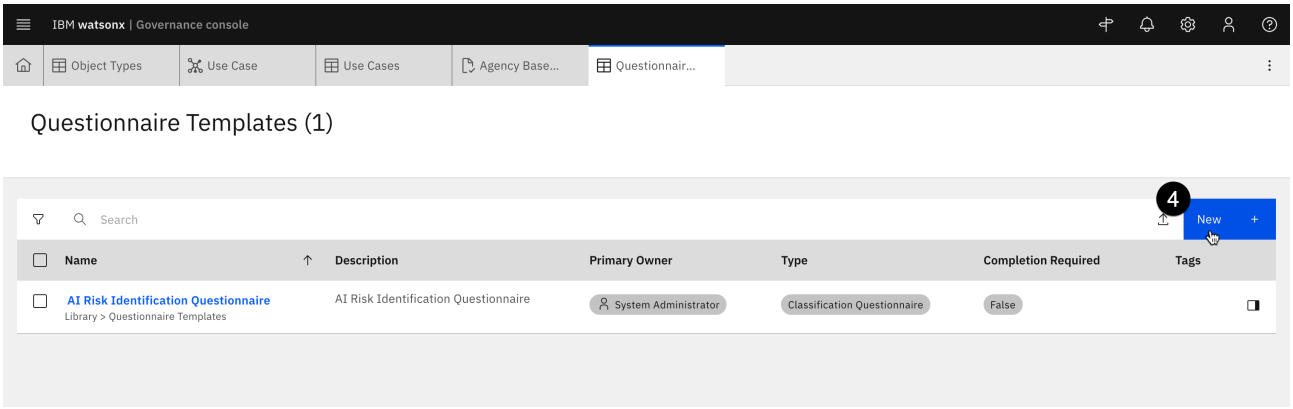
1. From the governance console, click the hamburger menu in the upper left.

2. Click on the Assessments menu item to expand it.

3. Click on the Questionnaire Templates menu item. Note that, depending on the current profile for your user, you may have more items listed in your menu. A new tab listing available templates opens.

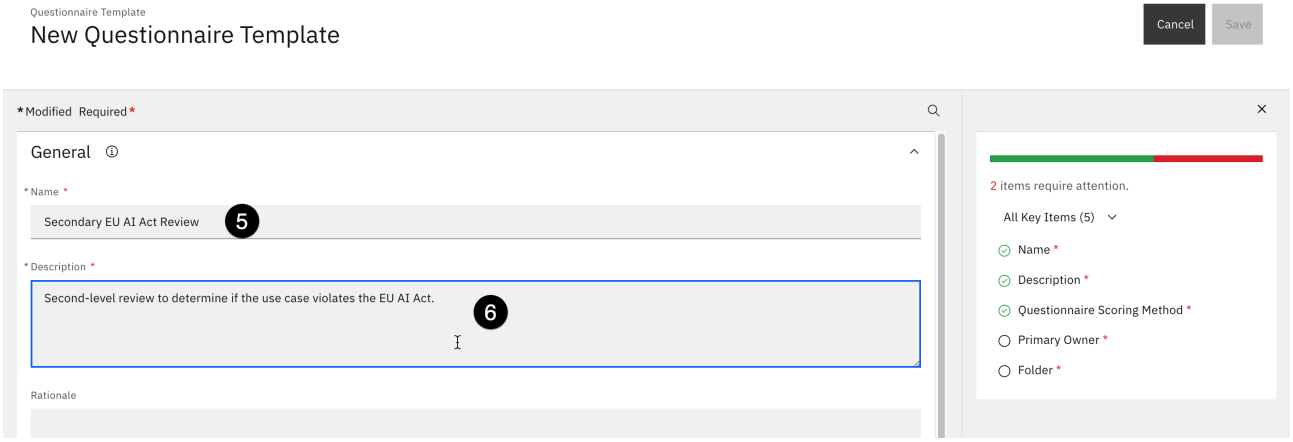


4. Click the New button in the upper right.



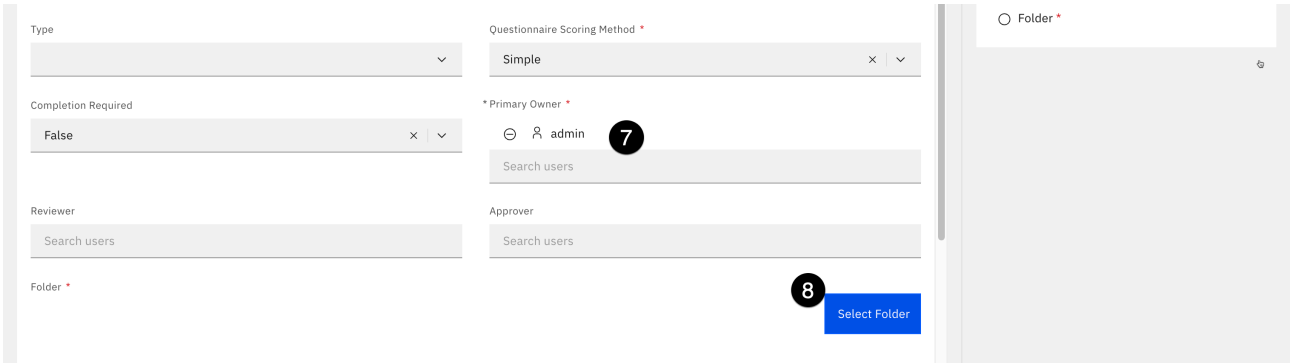
5. In the Name field, enter Secondary EU AI Act Review.

6. Enter a description in the Description field.



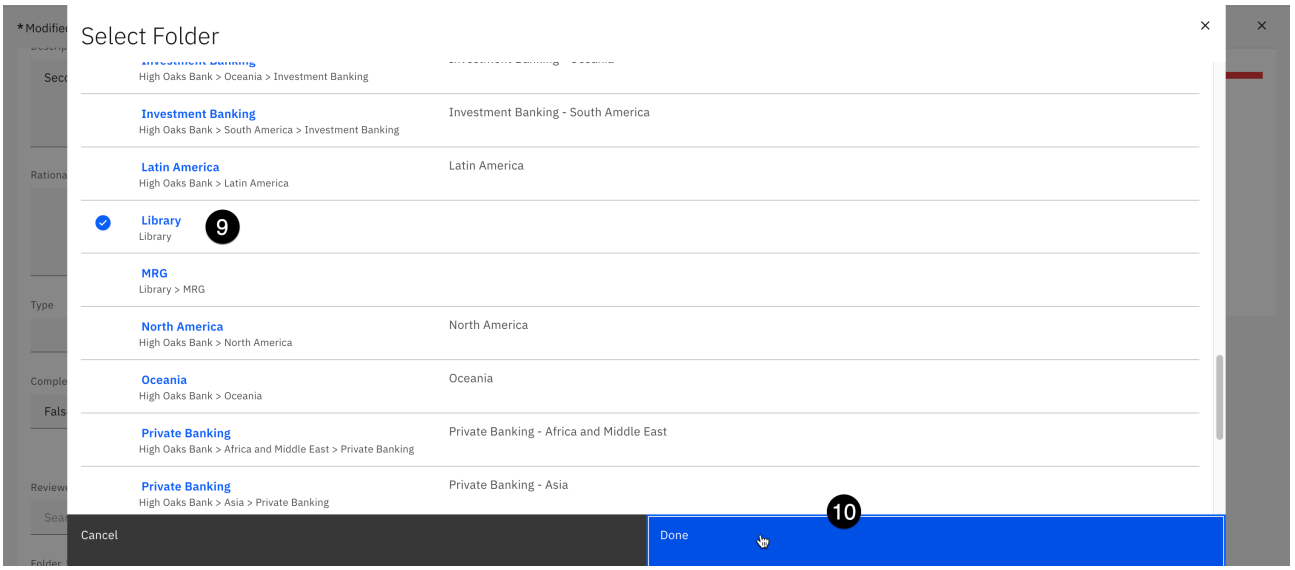
7. Enter the admin user in the Primary Owner field.

8. Click the Select Folder button. The folder selection dialog opens.



9. Scroll down in the table of folders and click on the Library folder.

10. Click the Done button. The dialog closes.



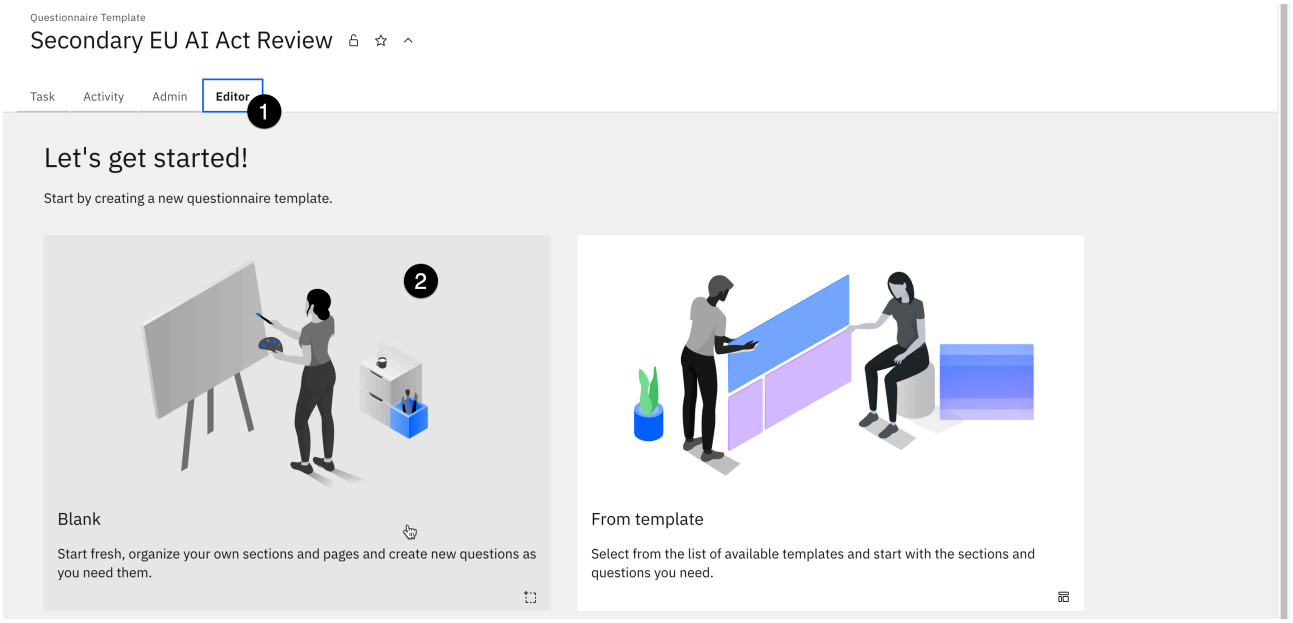
11. Click the Save button in the upper right to save the new questionnaire template. The Task view opens.

2. Add questions

Now that the questionnaire template has been created, you may add questions to it. In this example, you will create a very simple set of questions to reflect a larger review, but when performing a Proof of Experience (PoX), it can be valuable to allow the client to create their own questions that are relevant to their organization's requirements.

1. From the questionnaire template Task view, click on the Editor tab.

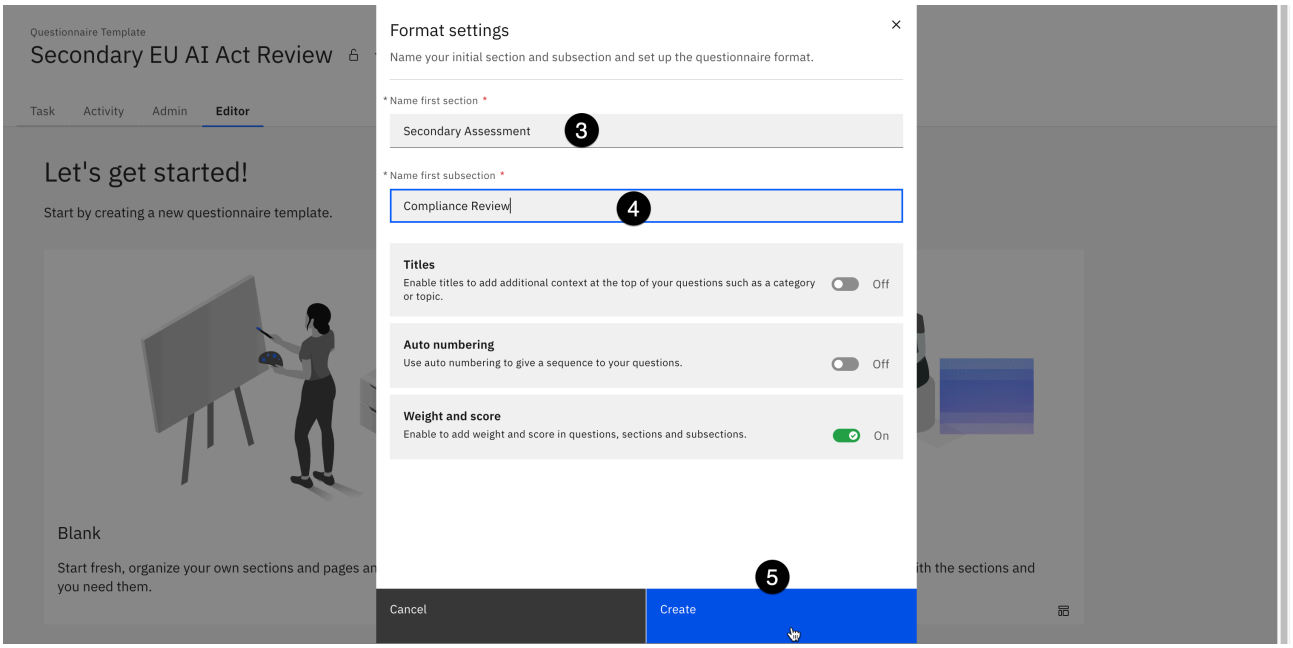
2. Click on the Blank tile to create questions from scratch. The Format settings dialog opens.



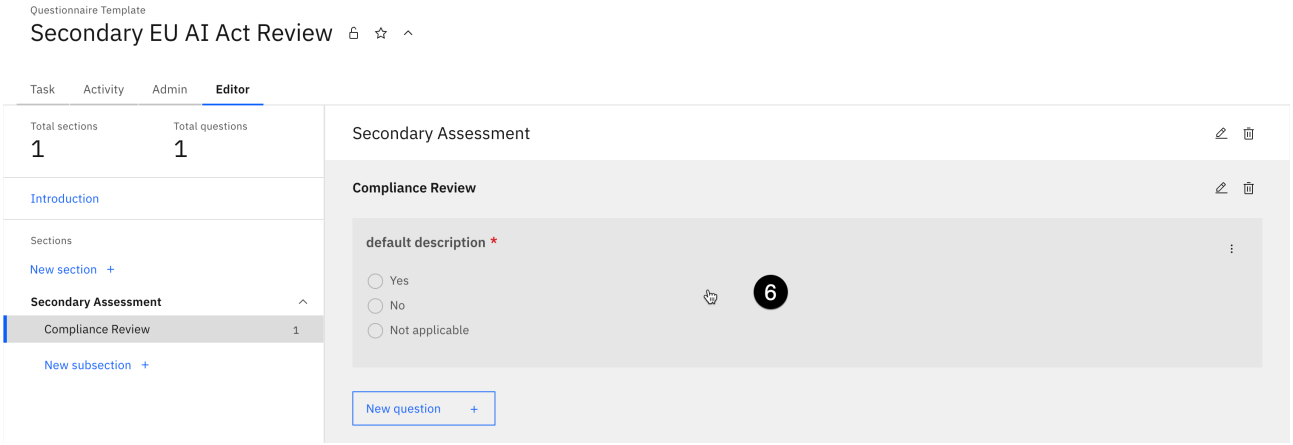
3. Enter Secondary Assessment in the Name first section field.

4. Enter Compliance Review in the Name first subsection field.

5. Click the Create button. Note that if you receive a Network error message, you may need to close the current tab, return to the Questionnaire Templates tab, and refresh the page. From this point, the new template should appear in the list. You can click on it and switch to the Editor tab on the template screen.



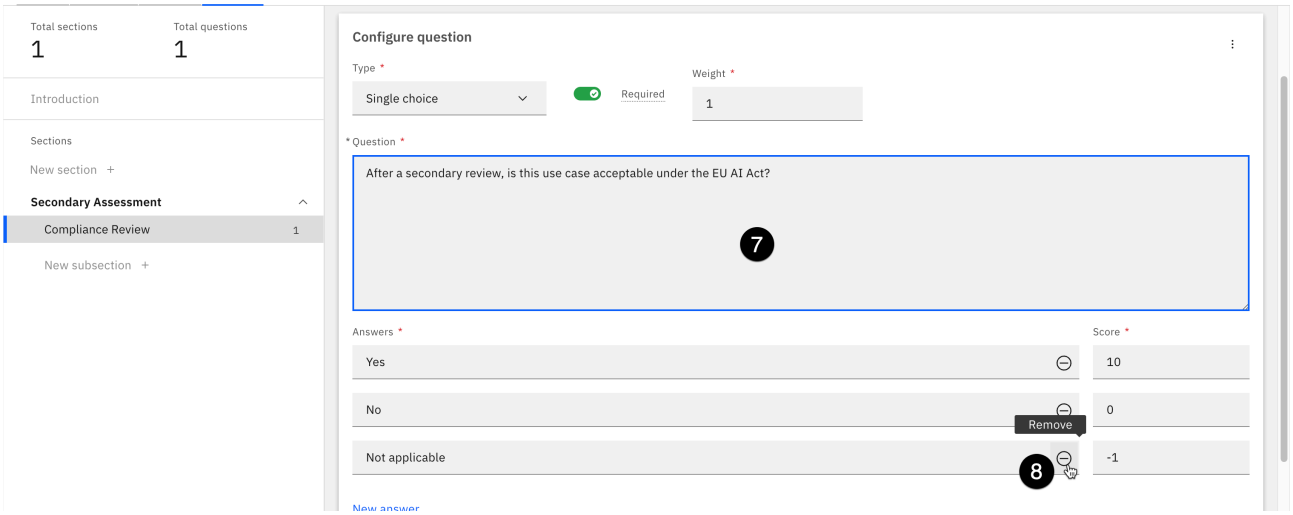
6. The template has been pre-populated with a default question. Click the question tile to edit it. The Configure question form opens.



7. Copy and paste the following text in the Question field, replacing the existing text:

```
After a secondary review, is this use case acceptable under the EU AI Act?
```

8. Click the Remove icon to the right of the Not applicable choice.



9. Take a moment to review the other possible actions you can take on this question. You have the ability to build display logic to determine when this question appears. You can add additional context, set up multiple choice questions, and more. Creating full in-depth questionnaires is beyond the scope of this lab, but familiarizing yourself with some of the options and allowing the client to build their own questionnaires can be helpful in a PoX.

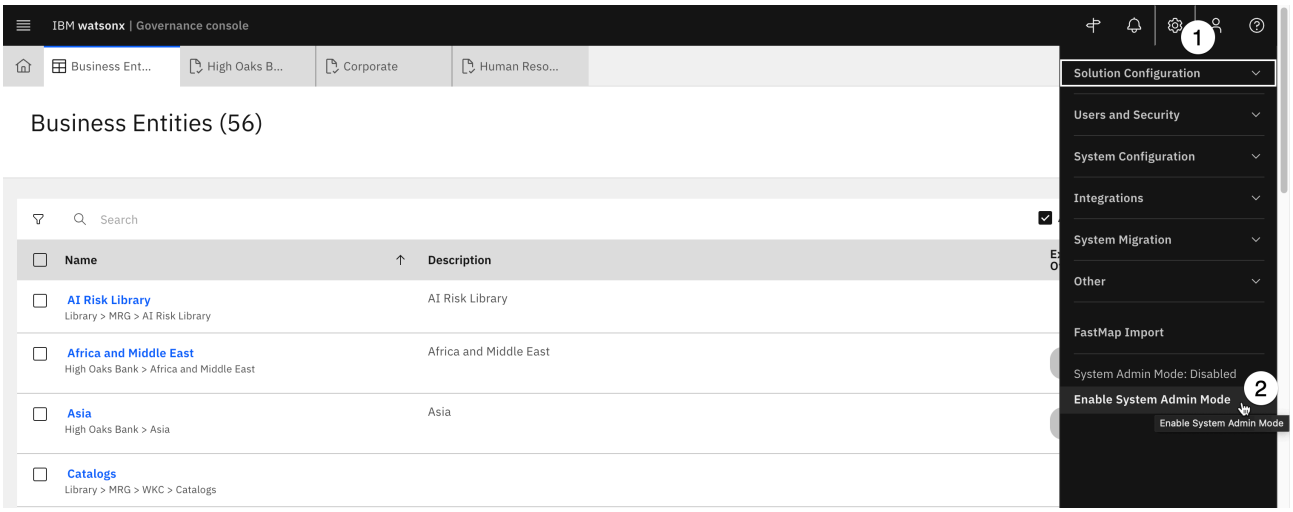
10. When you are finished exploring, click the gray area beneath the Configure question panel to save your changes. At this point, you may add additional questions as you wish. When you are satisfied with the questionnaire, you may proceed with the lab.

3. Add the questionnaire to the existing AI assessments

You have just created a new type of assessment for AI models. In order to incorporate it into AI-related workflows, you will need to make further configuration changes to add it to the list of existing AI assessments.

1. Click the gear icon in the upper right to open the Administration menu.

2. Click Enable System Admin Mode to enable changes.

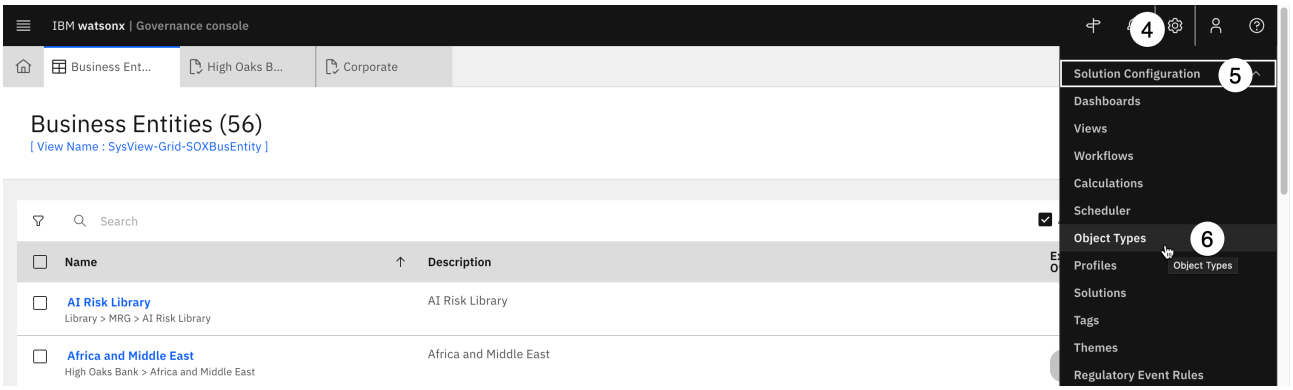


3. A popup window will open, prompting you to confirm your choice, and notifying you that while the mode is enabled, the system will be unavailable to other users. Click the Enable button to confirm.

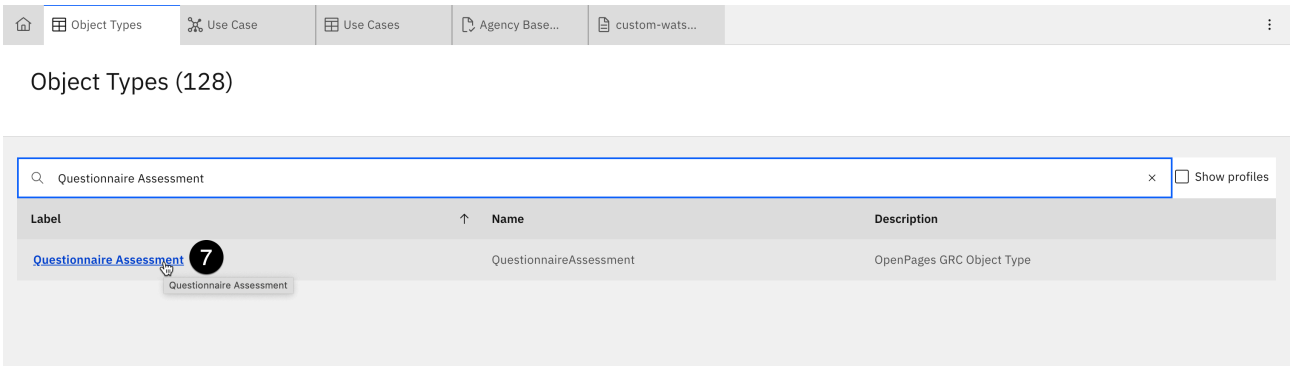
4. Click on the gear icon again to open the Administration menu.

5. Click on the Solution Configuration menu item to expand it.

6. Click on the Object Types menu item. The Object Types tab opens.

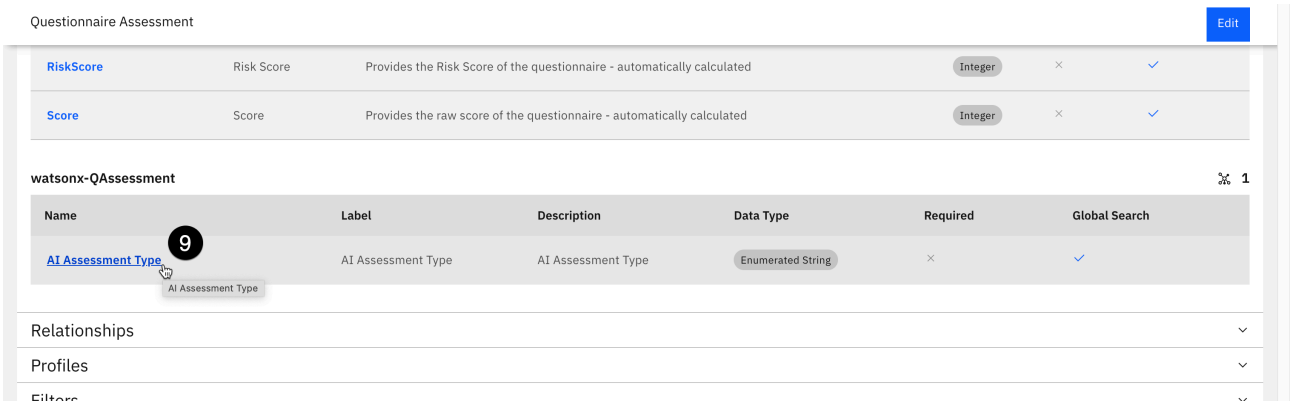


7. Enter Questionnaire Assessment in the search field to narrow the results of the table, then click on Questionnaire Assessment in the table.

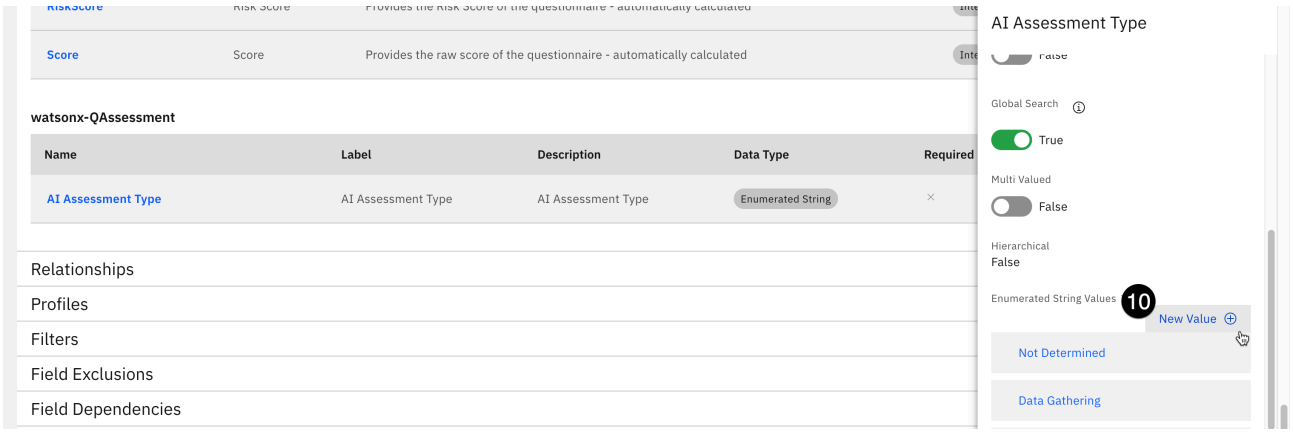


8. Click on the Fields section to expand it.

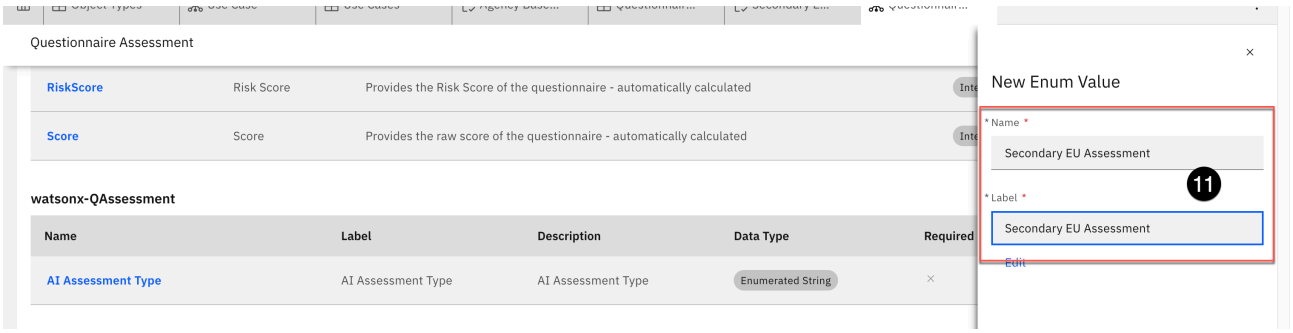
9. Scroll down to the watsonx-QAssessment section and click on the entry for AI Assessment Type. The field information panel opens.



10. In the information panel on the right, scroll down to the Enumerated String Values section and click on the New Value button.



11. Enter Secondary EU Assessment in both the Name and Label fields.



12. Click the Create button at the bottom right.

13. Click the Done button to save your change to the AI Assessment object.

14. Once the changes have saved, you can turn off System Admin mode. Click the gear icon in the upper right to open the Administration menu.

15. Click Disable System Admin Mode menu item, then click the Disable button in the confirmation dialog box that opens to confirm your choice.

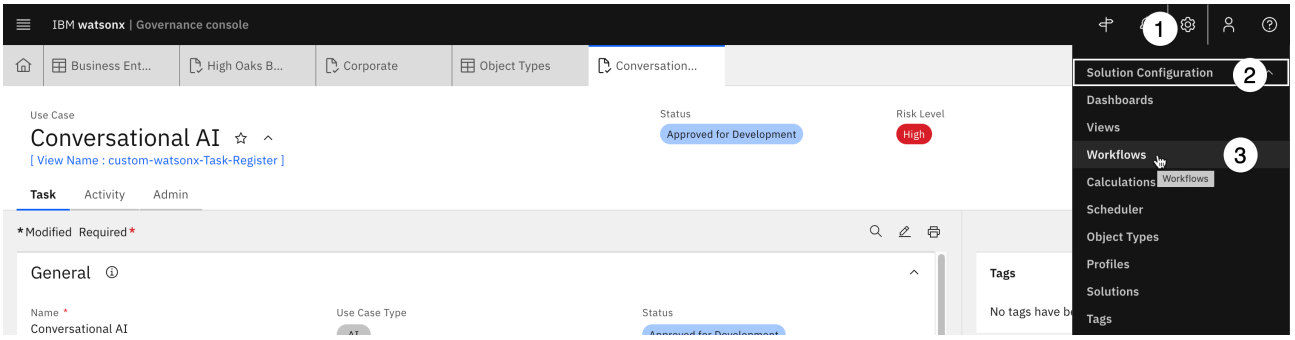
4. Update the AI assessment workflow

Now that you have created a new type of AI assessment, you will need to associate your assessment into the built-in workflow for AI use cases.

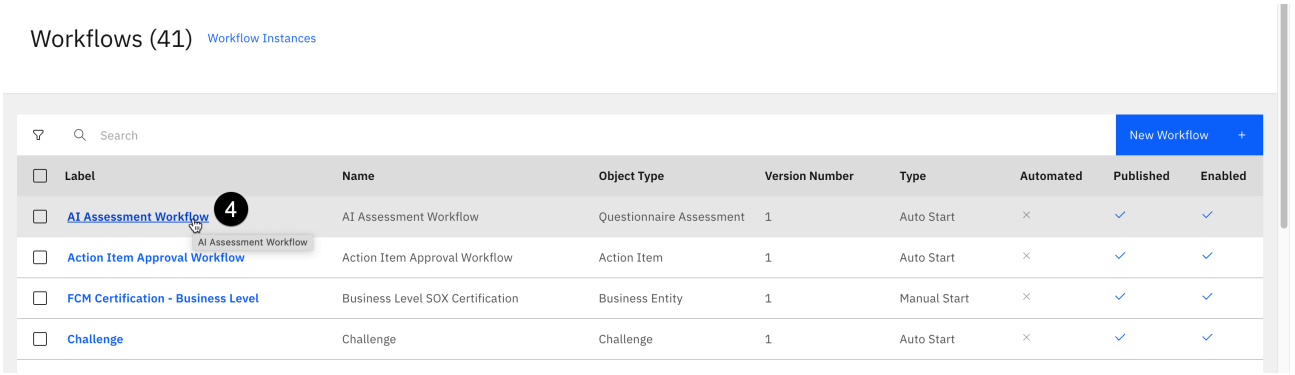
1. From the watsonx governance console, click the gear icon in the upper right to open the Administration window.

2. Click on the Solution Configuration menu item to expand it.

3. Click on the Workflows menu item. A new tab listing all the existing workflows opens. Note that you may receive a warning message about not having access to all of the items in the workflow; this can be ignored.

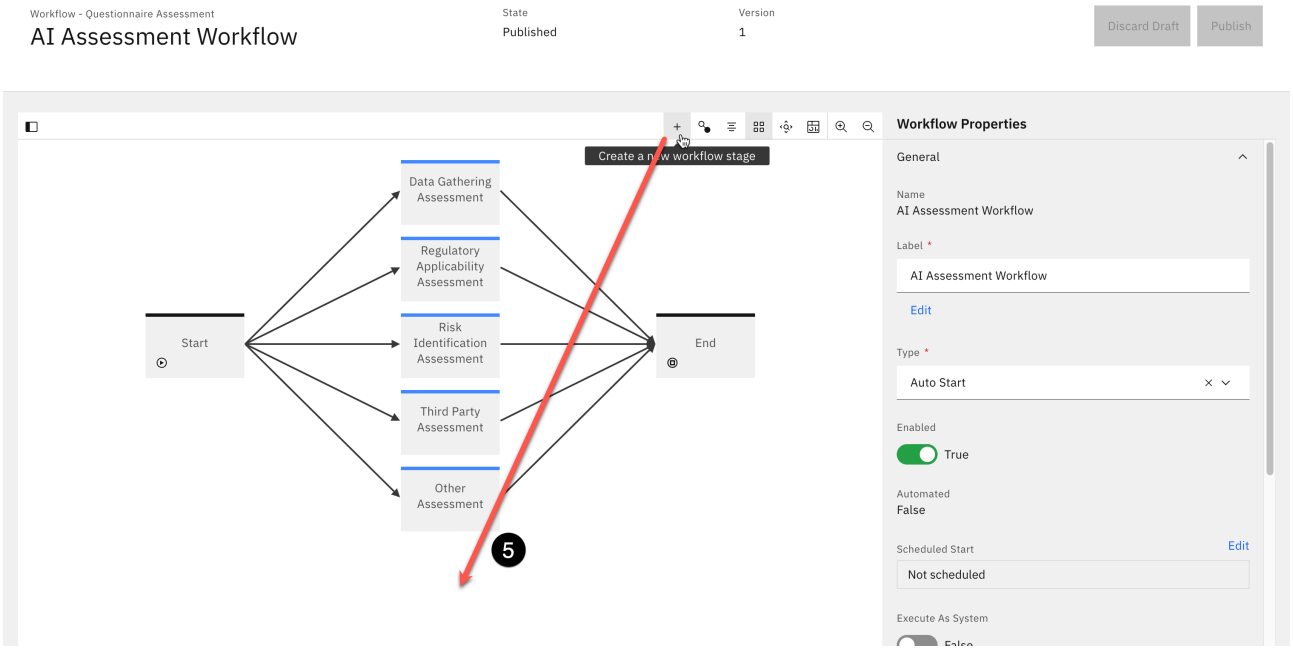


4. Click on the AI Assessment Workflow from the table. The editor palette opens, showing the different stages of the workflow.



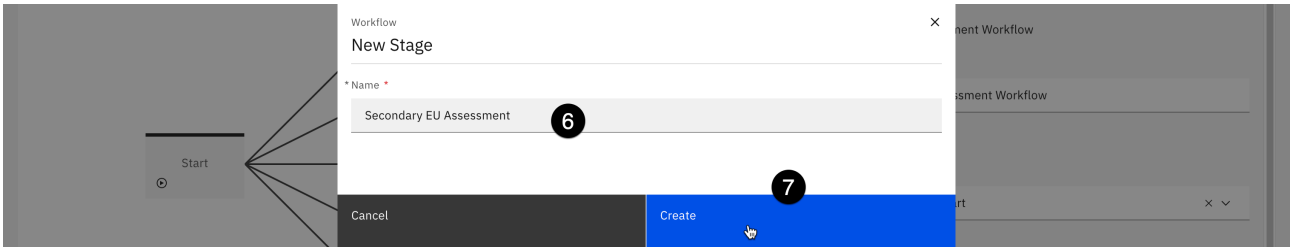
You will explore the editor in more detail in the next section, when you customize the Use Case Request workflow.

5. Locate the + icon in the upper right of the palette window. Click and drag it to beneath the Other Assessment box to create a new workflow stage. The New Stage dialog opens.

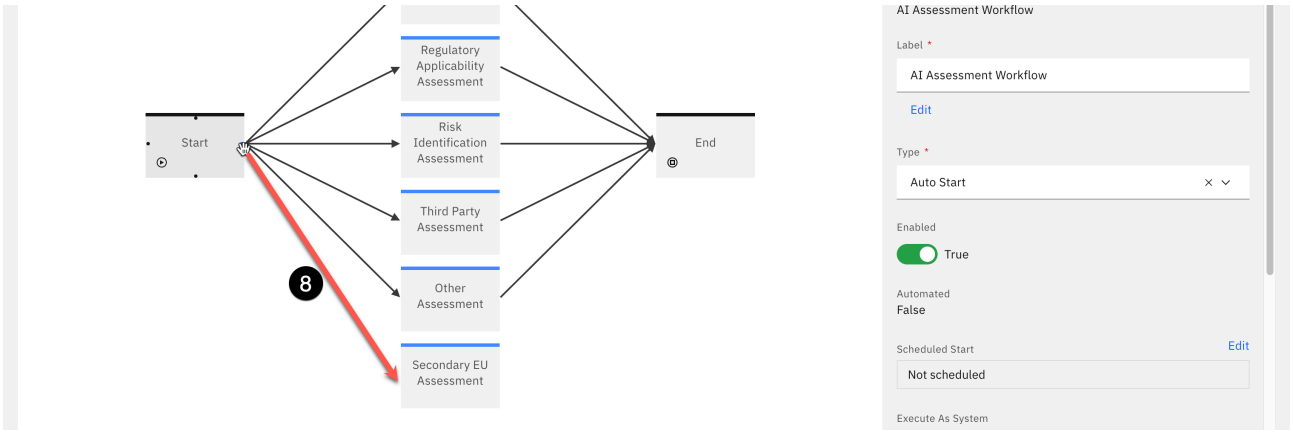


6. Enter Secondary EU Assessment in the Name field.

7. Click the Create button to create the stage, which will now appear on the palette.

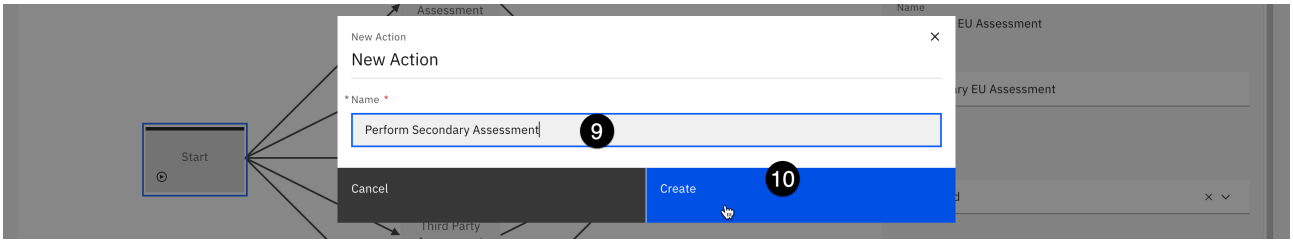


8. Hover your mouse pointer over the Start workflow stage to make four black boxes appear on the stage border. Click and drag one of the boxes to the new Secondary EU Assessment stage box to create an action linking the two stages. The New Action dialog opens.



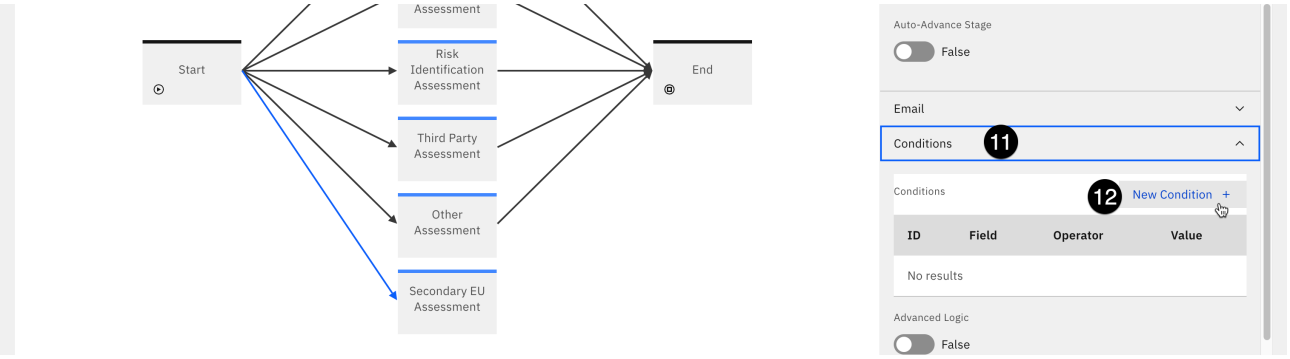
9. Enter Perform Secondary Assessment in the Name field.

10. Click the Create button to create the action and close the dialog.



11. In the Action Properties panel on the right, scroll down and click on the Conditions section to expand it.

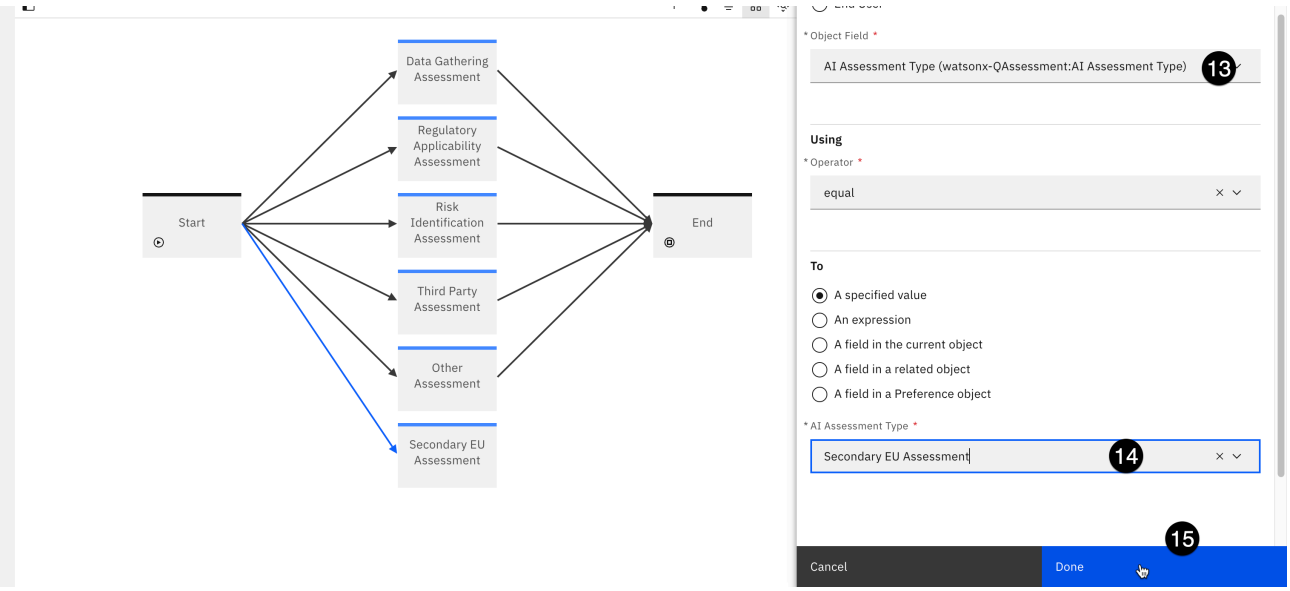
12. Click on the New Condition button. The Conditions panel opens.



13. Click on the Object Field dropdown and select AI Assessment Type... from the list.

14. Click on the AI Assessment Type dropdown and select Secondary EU Assessment from the list. This value appears in this list because you added it as an *Enumerated String Value* for AI Assessment Types in the previous step.

15. Click the Done button to save the condition. The Condition panel closes.



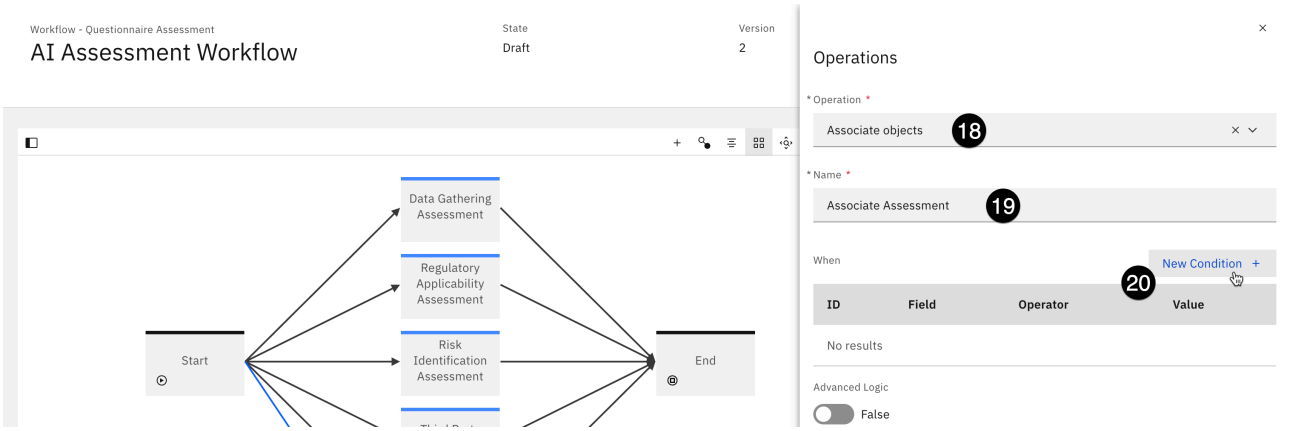
16. In the Action Properties panel on the right, scroll down and click on the Validations and Operations section to expand it.

17. Click on the New Operation button. The Operations panel opens.

18. Click on the Operation dropdown and select Associate objects from the list.

19. Enter Associate Assessment in the Name field.

20. Click on the New Condition button. The When condition panel opens.



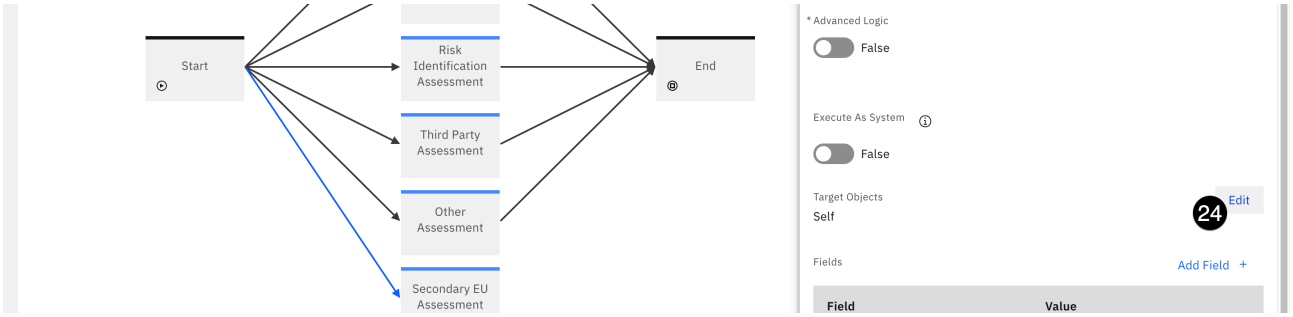
21. Click on the Object Field dropdown and select AI Assessment Type....

22. Click on the AI Assessment Type dropdown and select Secondary EU Assessment.

23. Click the Done button to close the When panel.

24. Click the Edit button to the right of Target Objects. The Target Objects panel opens.

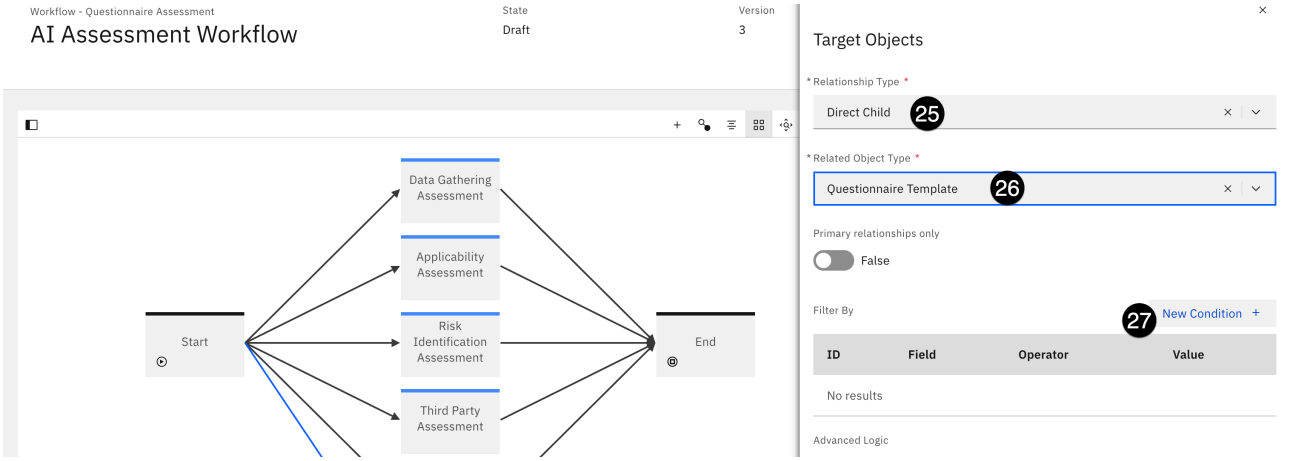
> Note: In some versions of the software, Target Objects may be called Objects to associate.



25. Click on the Relationship Type dropdown and select Direct Child from the list.

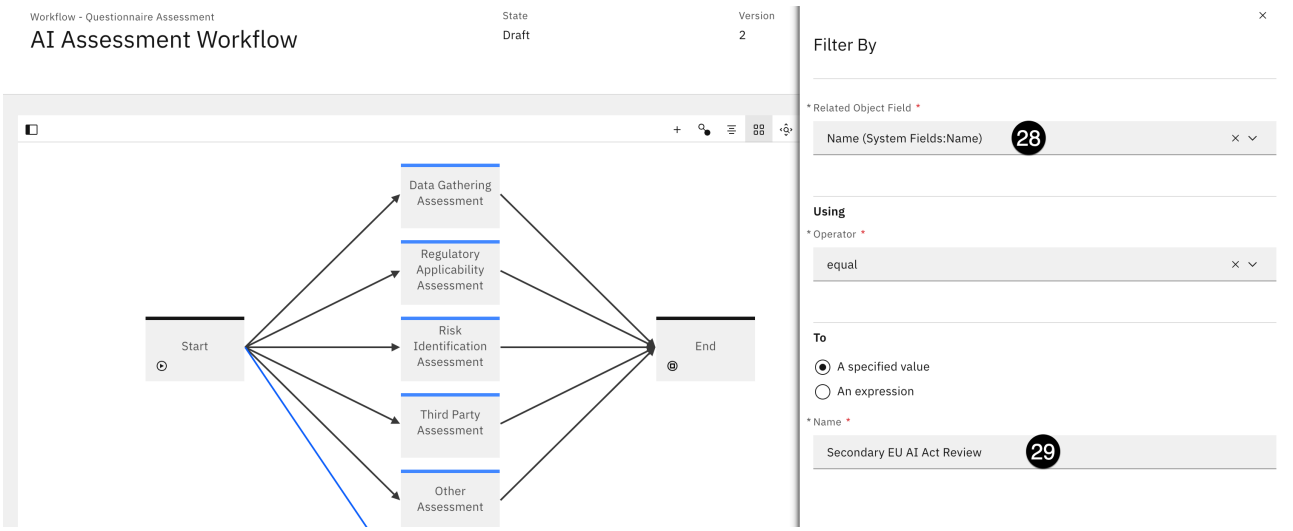
26. Click on the Related Object Type dropdown and select Questionnaire Template from the list.

27. Click on the New Condition button. The Filter By panel opens.



28. Click on the Related Object Field dropdown and select Name... from the list.

29. Enter the exact name of the questionnaire template you created in a previous step in the Name field. If you have been following the instructions, you named it Secondary EU AI Act Review.



30. Click Done to close the Filter By panel.

31. Click Done to close the Object to associate panel.

32. Click Done to close the Operations panel.

You have now linked the Start stage and the Secondary EU Assessment stage using an action. To complete the process, you must link the Secondary EU Assessment stage to the End stage.

33. Hover your mouse pointer over the Secondary EU Assessment stage box to make four black boxes appear on the stage border. Click and drag one of the boxes to End stage box to create an action linking the two stages. The New Action dialog opens.

34. Enter Assessment complete in the Name field and click the Create button to close the dialog.

35. Click the Publish button in the upper right of the screen to save your updates. Your new questionnaire has been added to the AI assessment workflow, and can now be integrated into the workflow for use case approval.

Every organization will have their own requirements and preferences when it comes to governance processes. In the governance console, a workflow represents a business process and describes the tasks involved in the process. The ability to fully configure and customize an automated workflow is one of the main differentiators for watsonx.governance. Many clients will be relying on manual processes that involve email approval chains between developers, risk assessors, and other stakeholders. Others will have attempted to awkwardly fit their existing organizational structure into pre-set approval workflows offered by some of our competitors.

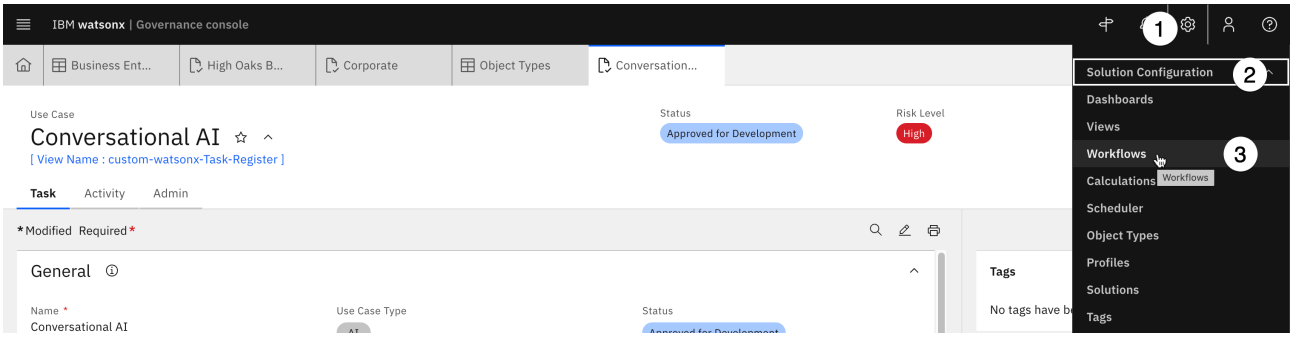
In this section of the lab, you will examine the workflow for a model use case request, and customize it. In this example, if the risk assessment questionnaire from the previous section results in a use case that is prohibited under the EU AI Act, the workflow will be configured to trigger a second-level audit by the compliance officer user you created earlier in the lab. As with all aspects of this lab, engaging with your client to alter the customization to fit their particular needs is a great way to demonstrate the flexibility of the solution.

5. Create workflow stages and actions

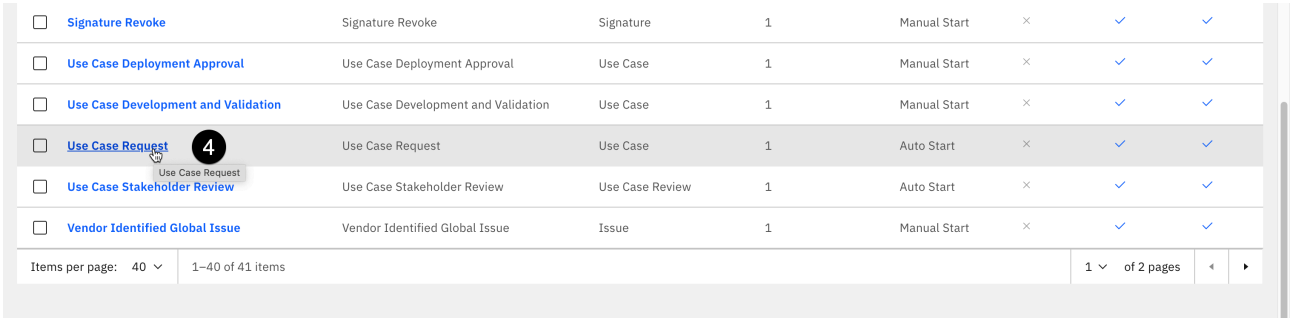
1. From the watsonx governance console, click the gear icon in the upper right to open the Administration window.

2. Click on the Solution Configuration menu item to expand it.

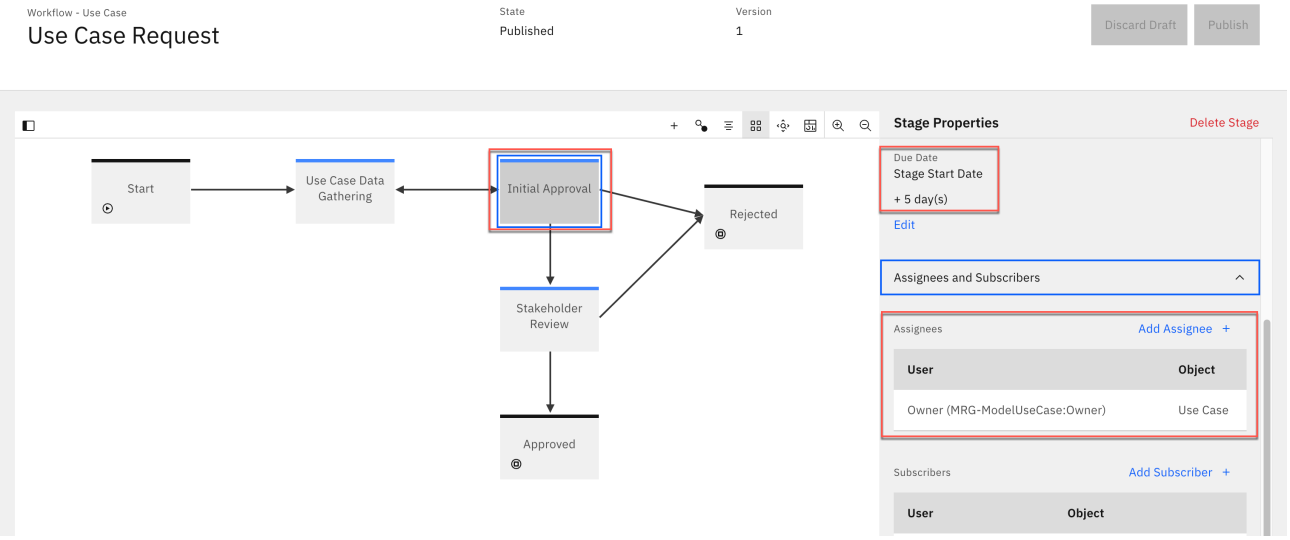
3. Click on the Workflows menu item. A new tab listing all the existing workflows opens. Note that you may receive a warning message about not having access to all of the items in the workflow; this can be ignored.



4. Locate Use Case Request in the table and click on it. The editor palette opens, showing the different stages of the workflow.



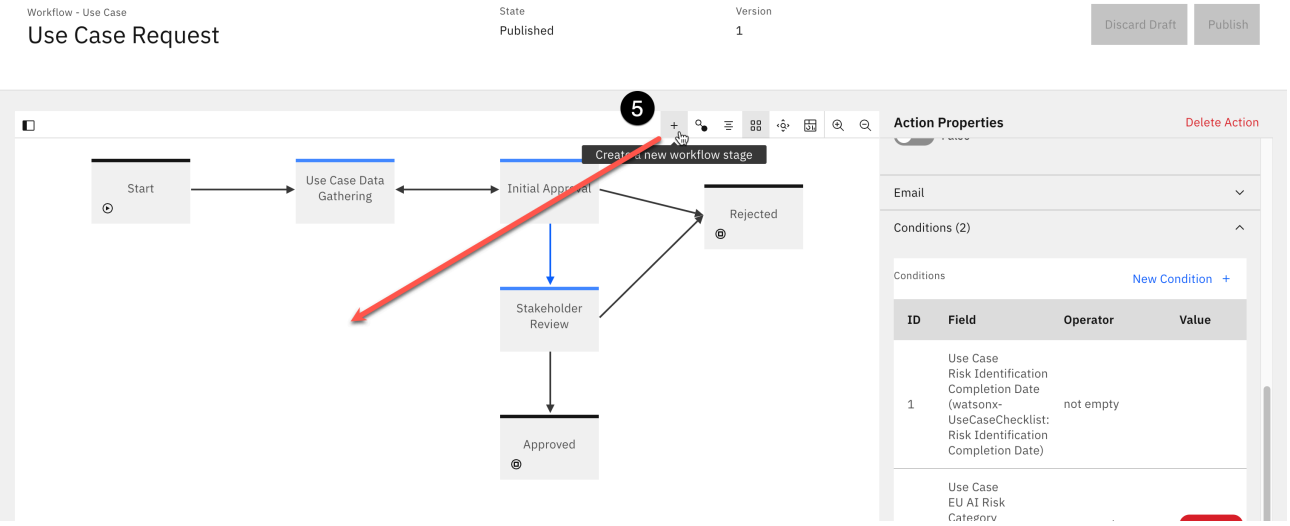
Take a moment to explore the items in the palette by clicking on them and observing the Workflow Properties panel on the right of the screen. For example, click on the Initial Approval box. Boxes represent stages of the workflow. In the properties panel, you can see that the due date of the action is set to five days after the stage start date. If you click on the Assignees and Subscribers section to expand it, you can see that the stage gets assigned to the use case owner.



Next, click on the arrow joining the Initial Approval stage and the Stakeholder Review stage. Arrows represent actions that transition the use case between stages. Click on the Conditions section of the properties panel to expand it, and note that the two conditions here are being to bring about this action. First, that the Use Case Risk Identification assessment has been completed. And second, that the Use Case EU AI Risk Category property generated by that questionnaire's results was not *Prohibited*. In plain language, after the use case passes initial approval, the owner would fill out the questionnaire to determine risk. If the use case is not deemed prohibited by the EU AI Act, then it can proceed to the individual stakeholder review.

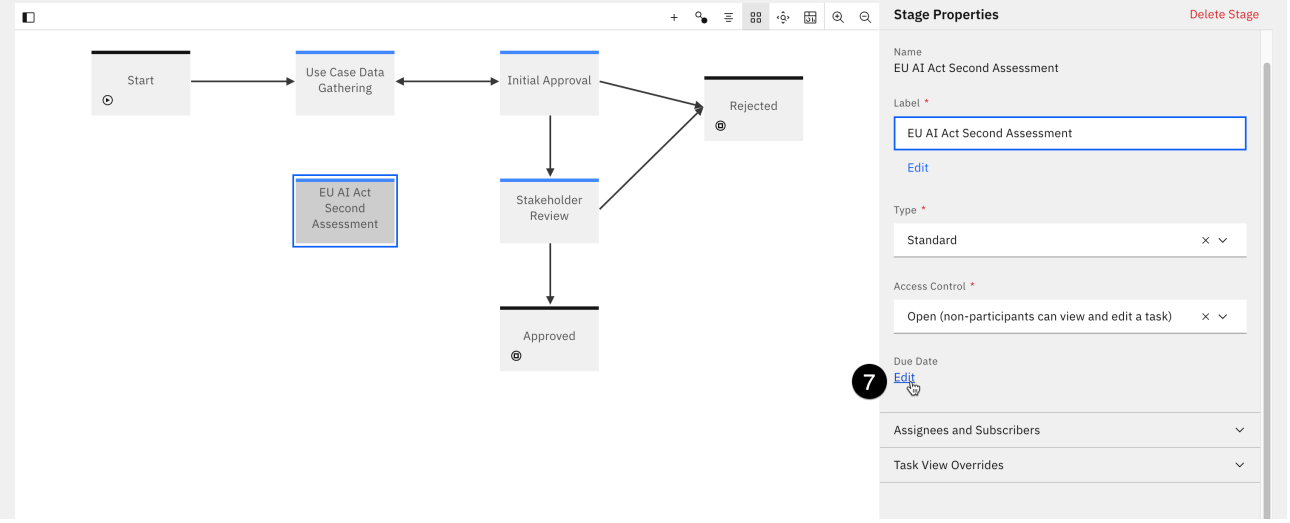
However, what if the organization wanted a second assessment in the case of a *Prohibited* result? In the steps below you will configure that as part of the workflow.

5. Locate the + icon on the palette toolbar, then click and drag it to the area on the palette shown below to create a new workflow stage. The New Stage dialog opens.



6. Enter EU AI Act Second Assessment in the Name field and click Create. The stage now appears on the palette.

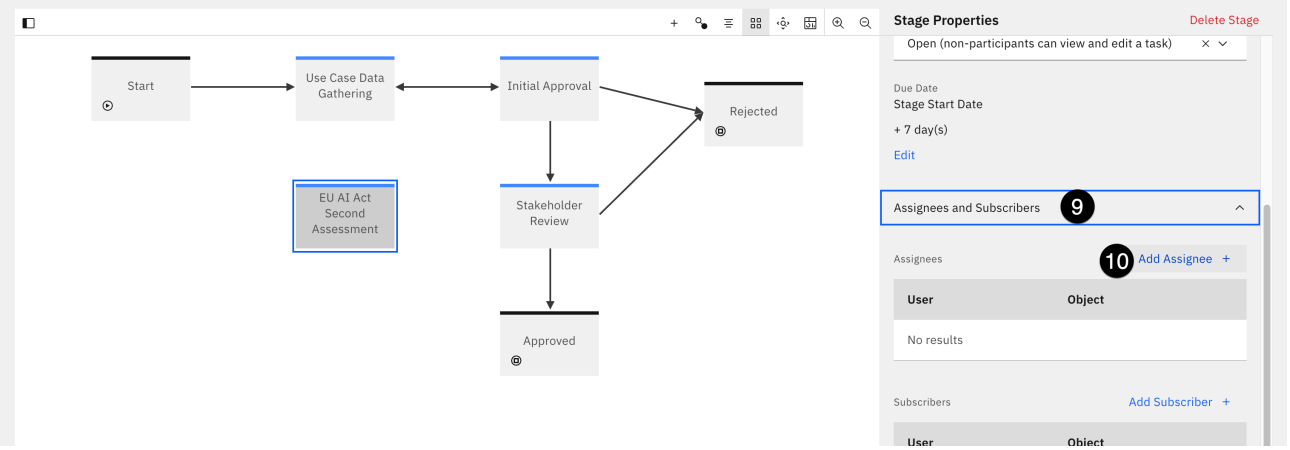
7. In the Stage Properties panel, click the Edit button below the Due Date.



8. Note the different options for setting the due date, and the flexibility provided by the governance console. Set the Number Of Days field to 7 to give the reviewer one week to perform the action, and click Done.

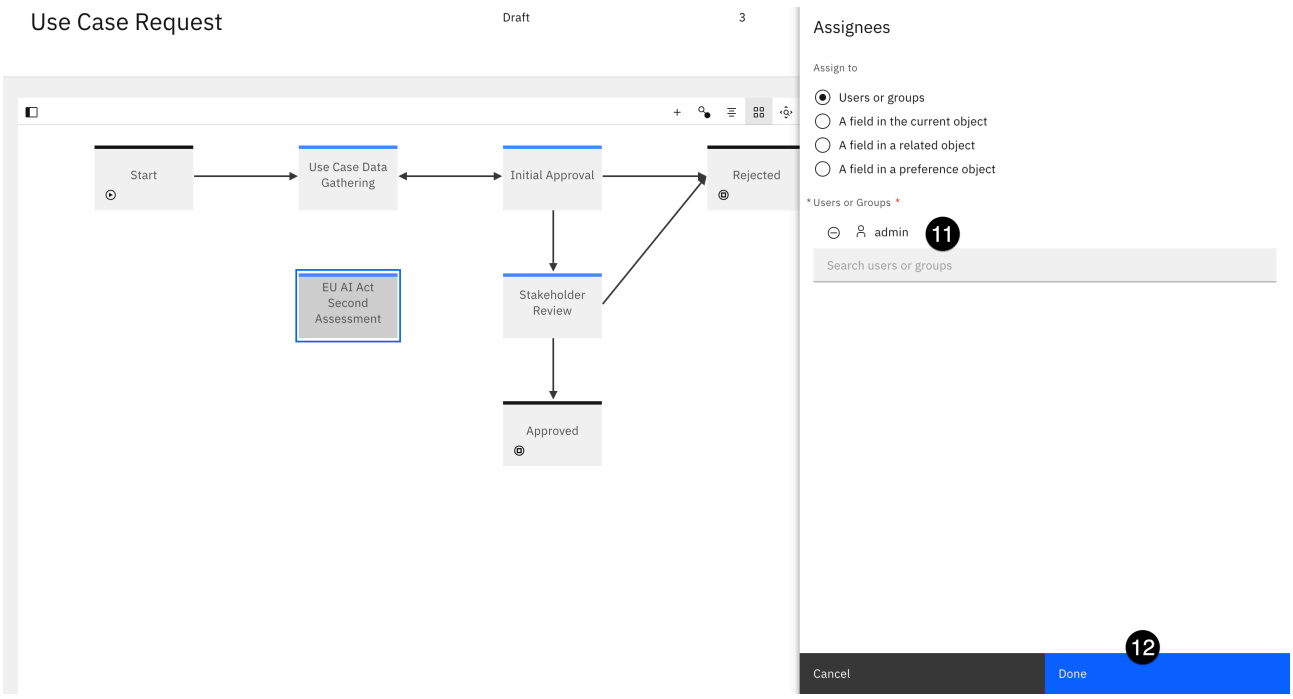
9. In the Stage Properties panel, click on the Assignees and Subscribers section to expand it.

10. Click on the Add Assignee button. The Assignees panel opens.



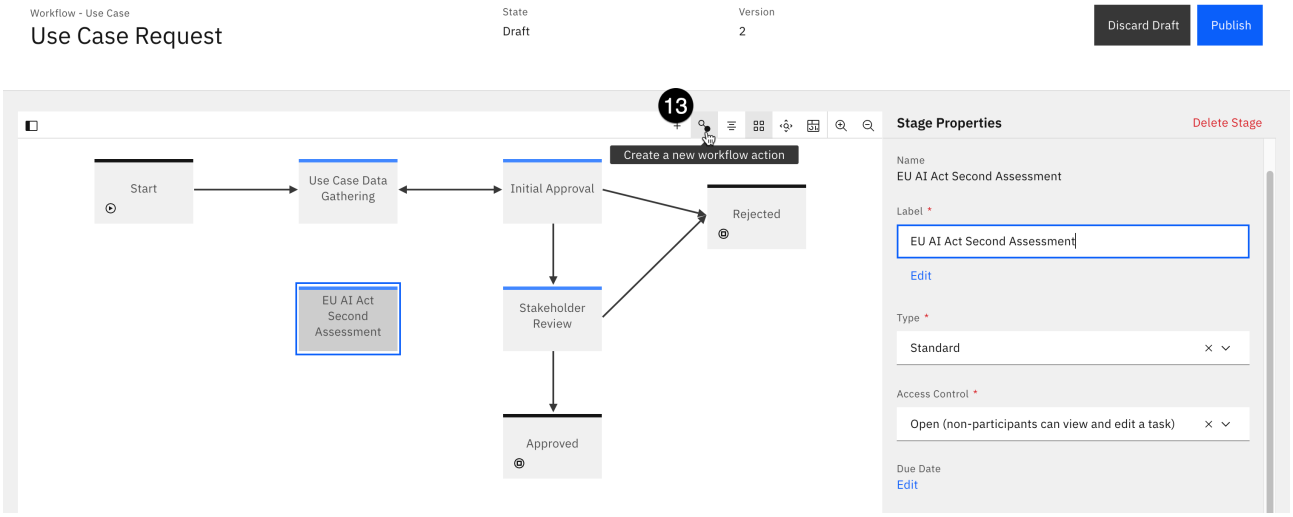
11. In the Users or Groups field, enter admin and select the admin user to assign them to this task. Note that in a real-world example, you would likely have created a group of compliance officers and assigned this task to them, as opposed to one specific user.

12. Click Done.



The workflow stage has been created. Next, you will add actions to trigger it.

13. Locate the Create a new workflow action button on the palette toolbar to the right of the + icon and click it. The New Action dialog opens.

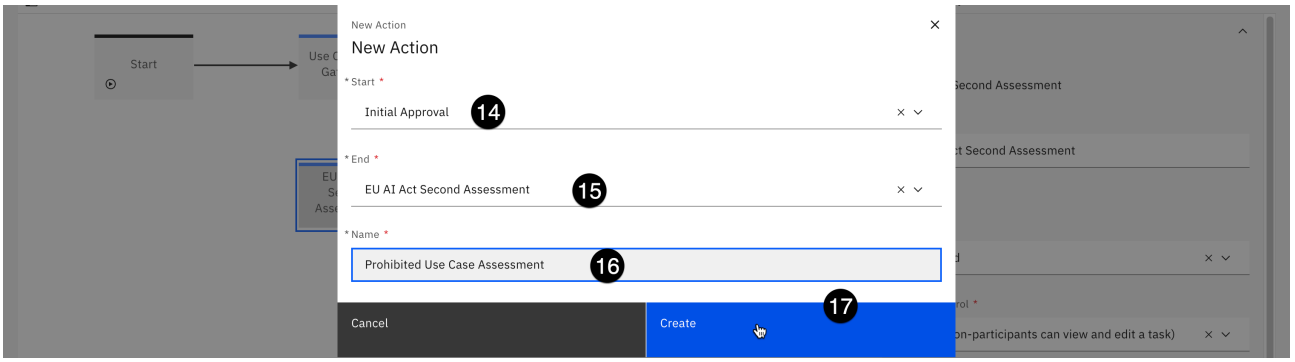


14. Click the Start dropdown and select the Initial Approval stage.

15. Click the End dropdown and select the EU AI Act Second Assessment stage you just created.

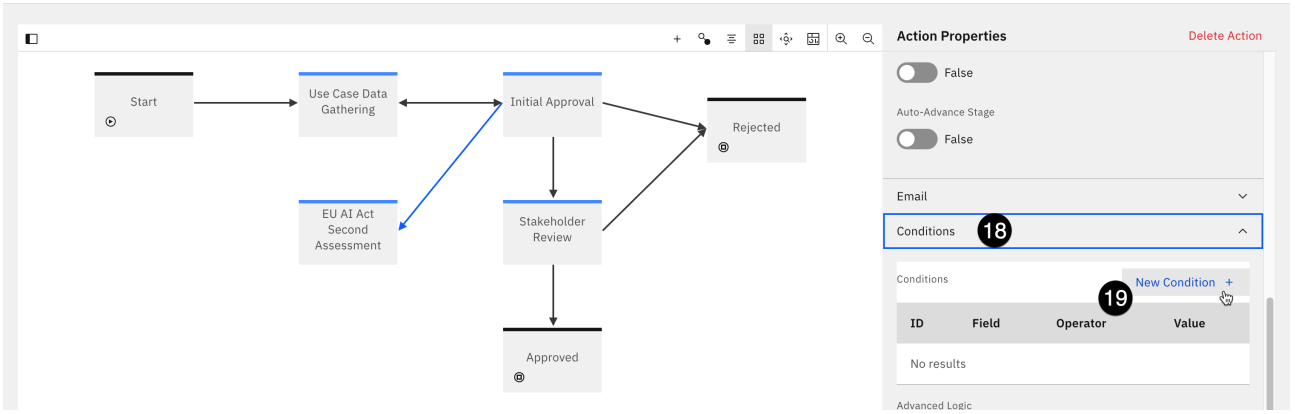
16. Enter Prohibited Use Case Assessment in the Name field. The text you enter into this field will appear as an available action in the Actions menu in the model use case view when the use case is in this stage.

17. Click Create. The action now appears as an arrow linking the Initial Approval stage with the EU AI Act Second Assessment stage.



18. In the Action Properties panel on the right, scroll down to the Conditions section and click on it to expand it.

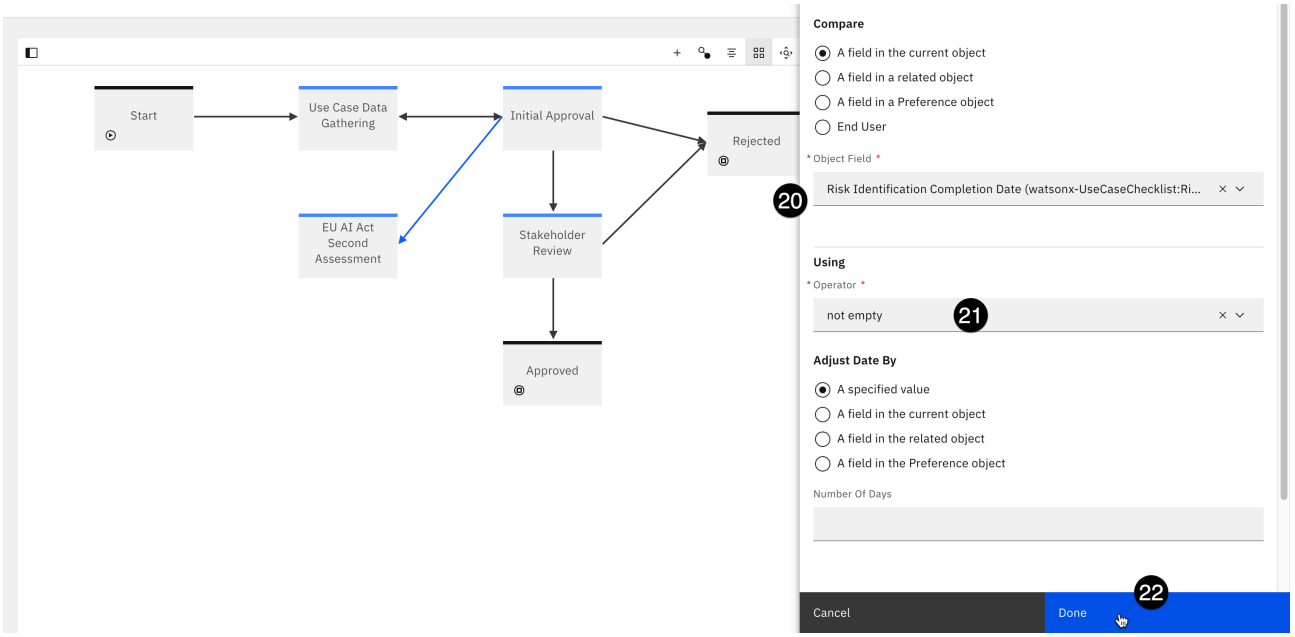
19. Click on the New Condition button. The Conditions panel opens.



20. Click on the Object Field dropdown and select Risk Identification Completion Date....

21. Click on the Operator field and select not empty to designate that the completion date of the Risk Identification assessment has a value, meaning that the questionnaire has been filled out.

22. Click Done to add the condition.



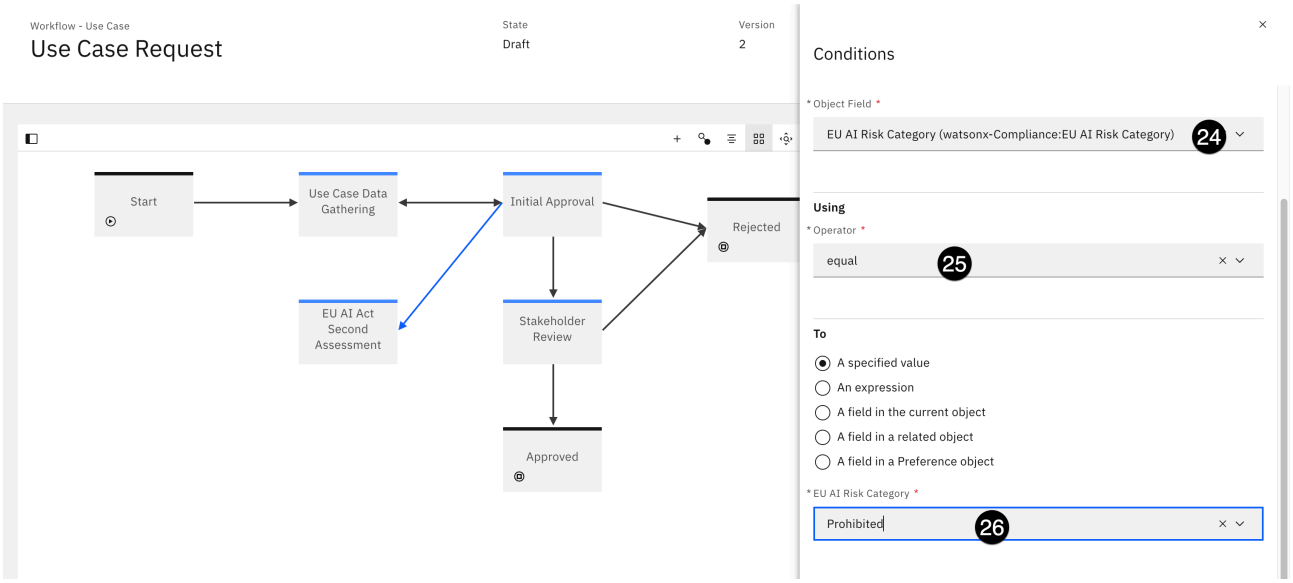
23. Click the New Condition button again to add a second condition.

24. Click on the Object Field dropdown and select EU AI Risk Category....

25. Click on the Operator dropdown and select equal.

26. Click on the EU AI Risk Category and select Prohibited.

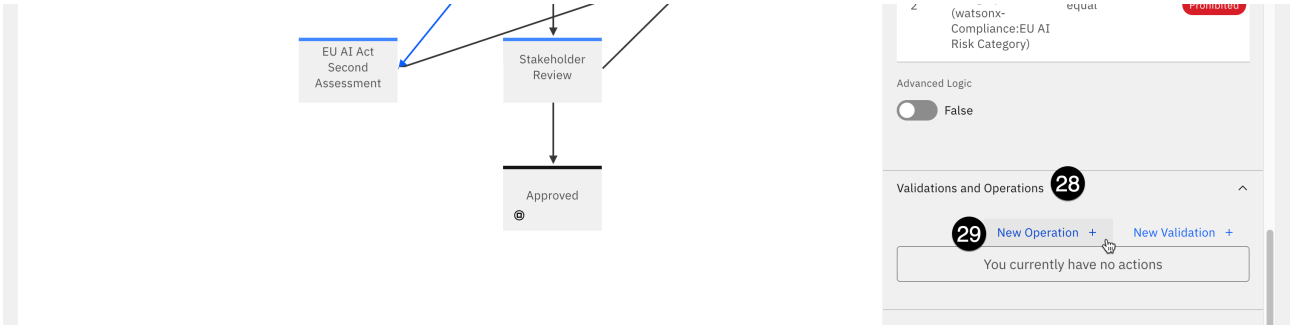
27. Click Done to add the condition.



The conditions for the action have been set so that it will trigger correctly. Next, you will need the action to automatically create the questionnaire for the secondary reviewer to fill out. In previous steps, you drafted questions for the form, and added the questionnaire to the AI assessment workflow. Taking those steps allows you to insert the new questionnaire into the current use case request workflow as operations that your action can take.

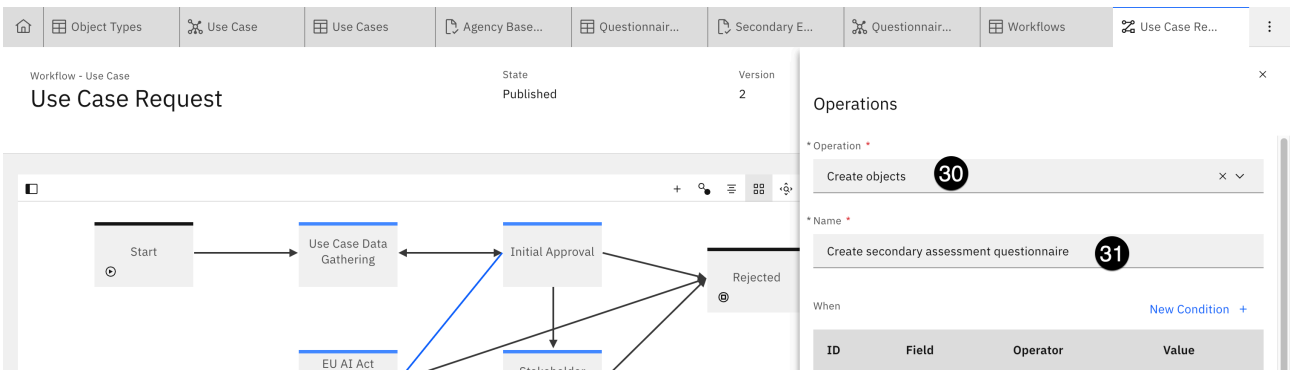
28. In the Action Properties panel, click on the Validations and Operations section to expand it.

29. Click on the New Operation button. The Operations panel opens.



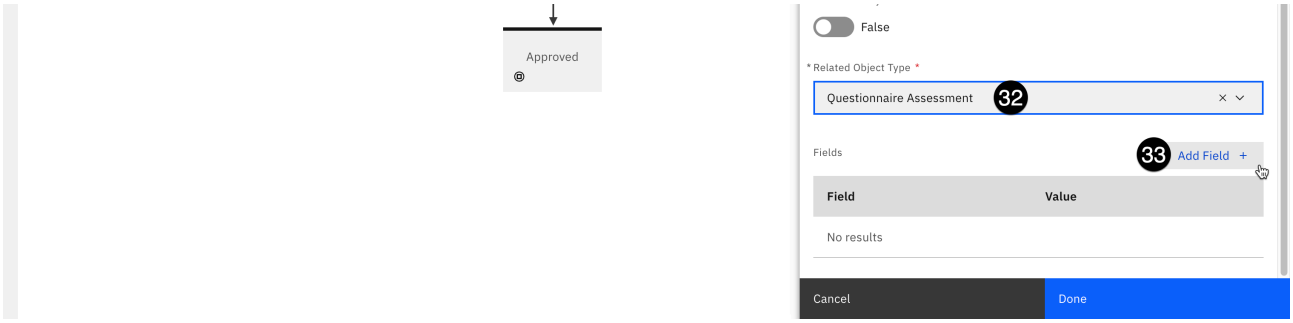
30. Click on the Operation dropdown and select Create objects.

31. Enter a description like Create secondary assessment questionnaire in the Name field.



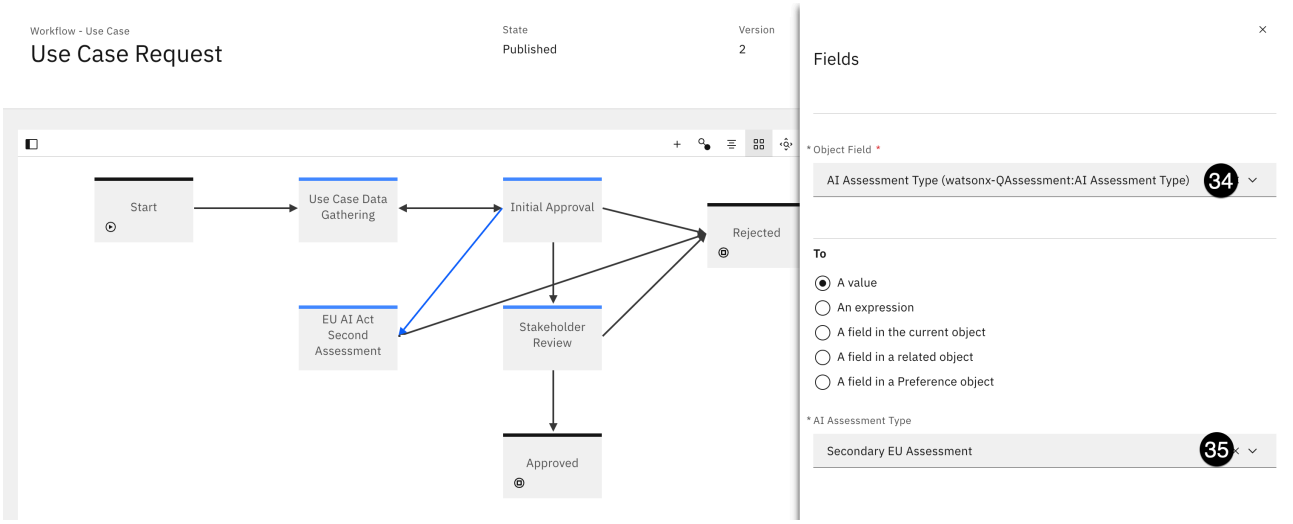
32. Scroll to the bottom of the Operations panel. Click on the Related Object Type dropdown and select Questionnaire Assessment.

33. Click the Add Field button. The Fields panel opens.



34. Click on the Object Field dropdown and select AI Assessment Type....

35. Click on the AI Assessment Type dropdown and select Secondary EU Assessment. This assessment type is visible because you added it to the AI assessment workflow in the previous step.



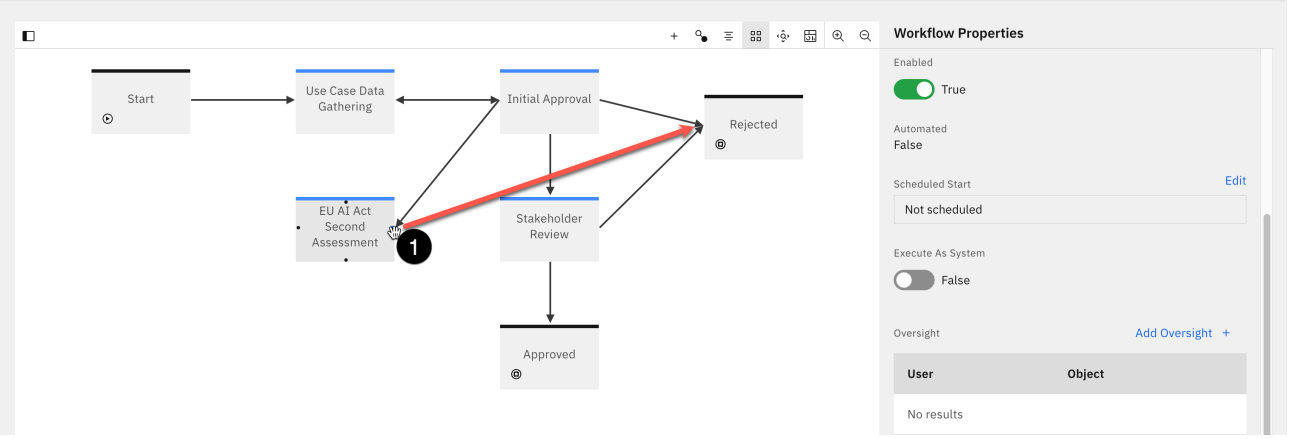
36. Click the Done button in the lower right to close the Fields panel.

37. Click the Done button to close the Operations panel.

At this point, you have created a new workflow stage, an automated action to trigger that stage, and an action to prompt a stakeholder with your newly-created questionnaire. However, the stage also needs resolution actions. The secondary reviewer must be able to either confirm the questionnaire assessment that the use case is prohibited under the EU AI Act and reject it, or overrule the questionnaire assessment and send it to the next stage of the workflow (Stakeholder Review).

6. Add resolution actions

1. Hover your mouse the EU AI Act Second Assessment stage; four black dots appear on the borders of the stage box. Click and drag one of the dots from the stage over to the Rejected stage on the palette to create an action linking the two. The New Action dialog appears.

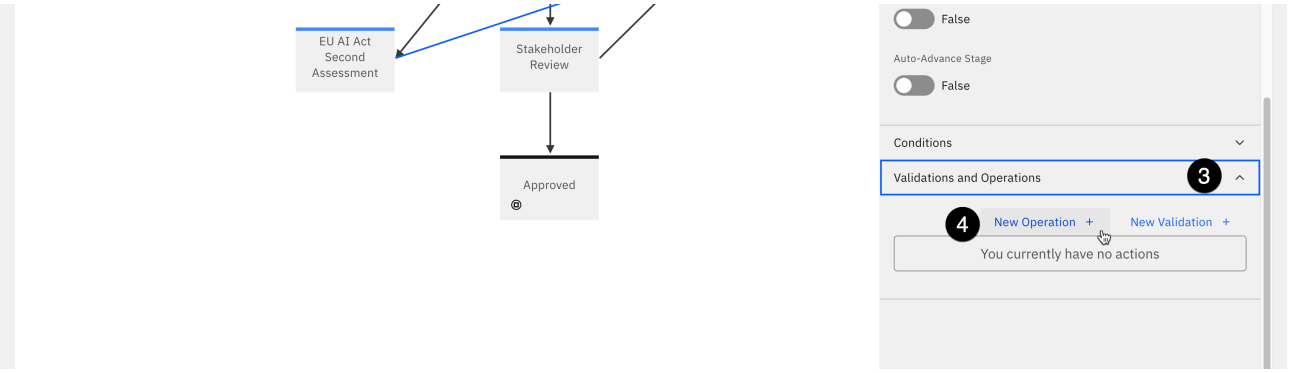


2. Enter Reject Use Case in the Name field and click Create. This value is what will appear in the user interface for the stage owner for them to reject the use case.

In addition to conditions, actions can also have operations assigned to them. In this example, you will set the use case status to Rejected.

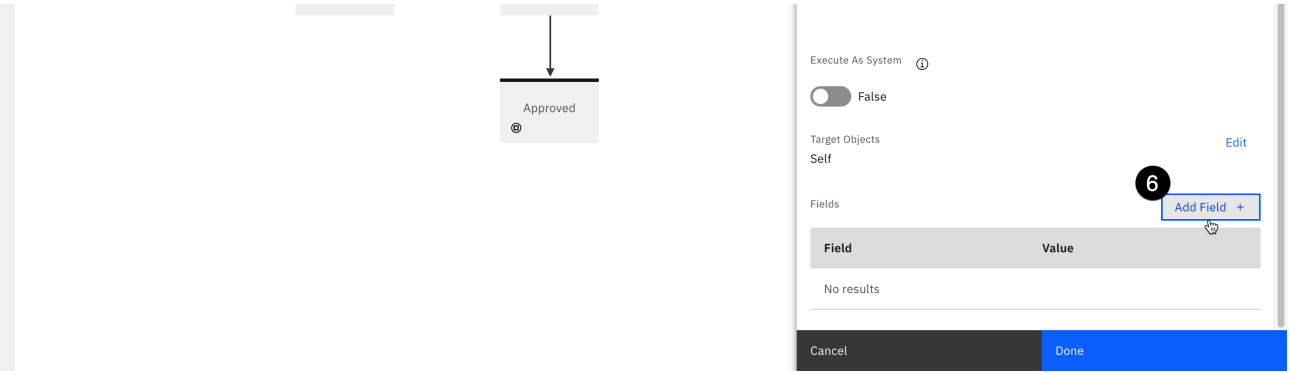
3. In the Action Properties panel, scroll down the bottom and click on the Validations and Operations section to expand it.

4. Click on New Operation. The Operations panel opens.



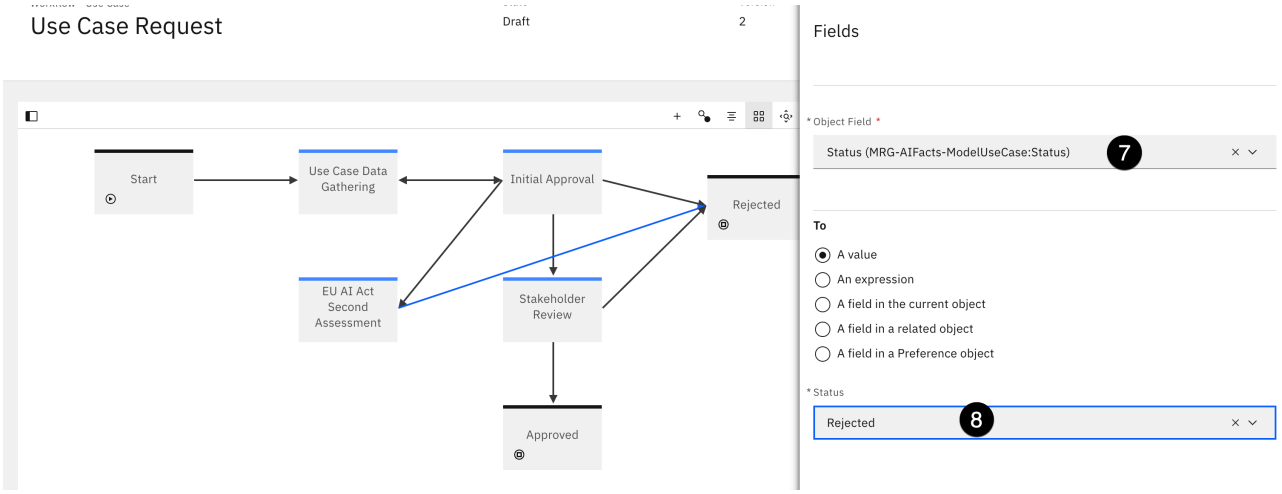
5. Enter Set status as rejected in the Name field.

6. Scroll to the bottom of the panel and click the Add Field button.



7. Click on the Object Field dropdown and select Status (MRG-AIFacts-ModelUseCase:Status).

8. Click on the Status dropdown and select Rejected.

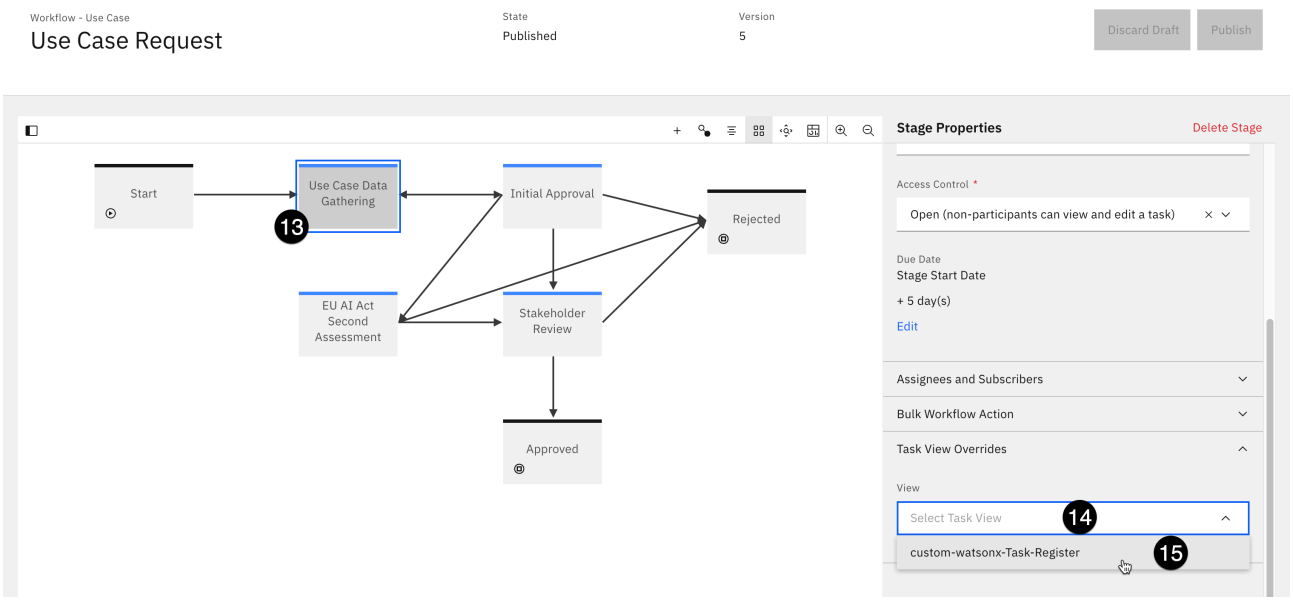


9. Click Done to create the field on the operation.
10. Click Done again to set the operation on the action. Performing the action will now update the model status.
11. Repeat step 1 above, clicking and dragging from the EU AI Act Second Assessment stage to the Stakeholder Review stage to create an action linking the two.
12. Enter Approve to Stakeholder Review in the Name field and click Create.

Note that the action linking the Initial Approval and Stakeholder Review stages has seven operations it performs, which you can see by clicking on it and expanding the Validations and Operations section of the properties panel. These operations prompt use case reviews from different departments before the final use case is approved. In a real-world example, you would duplicate these operations on the action you just created to link the EU AI Act Second Assessment and Stakeholder Review stages, since this represents the same level of approval. However, for the sake of brevity, this lab will not go over adding the operations to the new action. You may do so if you wish.

Finally, because you made changes to the default use case view, you will need to update the workflow stages, since they reference the view. Failure to update the stages will cause errors when a use case request goes through the workflow.

13. Click on the Use Case Data Gathering stage in the workflow. The Stage Properties panel opens.
14. Scroll to the bottom of the Stage Properties panel and click on the Task View Overrides section to expand it.
15. Click on the Select Task View dropdown and select the customized view you modified in previous steps from the list.



16. Repeat steps 13-15 for the three other stages intermediate stages in the workflow (it is not necessary for the Start, Rejected, or Approved stages).

17. When you are finished, click the blue Publish button in the upper right to publish your changes to the workflow.

Now that the use case request workflow has been modified, you will need to make one further customization to be able to approve a use case request for development.

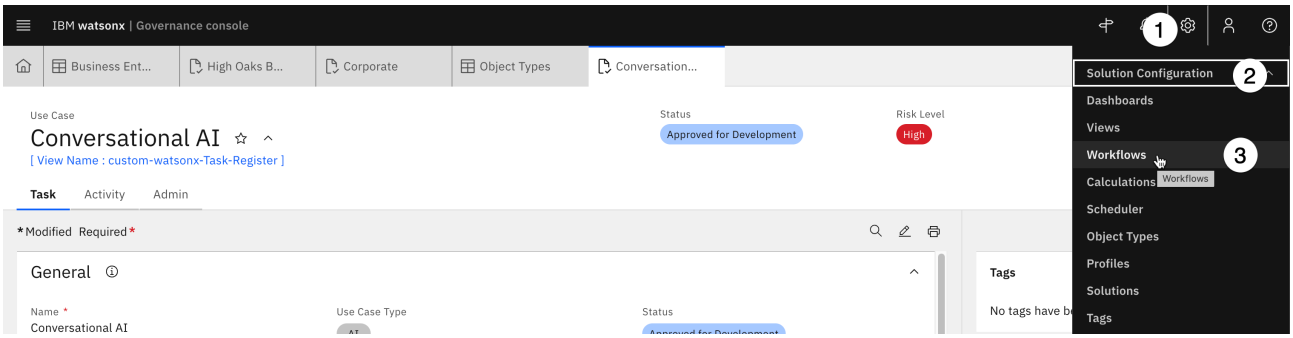
7. Update the stakeholder review workflow

In the current workflow, the final stage before a use case request is approved for development is the Stakeholder Review. In a real world situation, an organization would assign this review to members of the business entity that requested the use case, risk managers, or other stakeholders. For the sake of this lab, you will assign the stakeholder review to the use case owner.

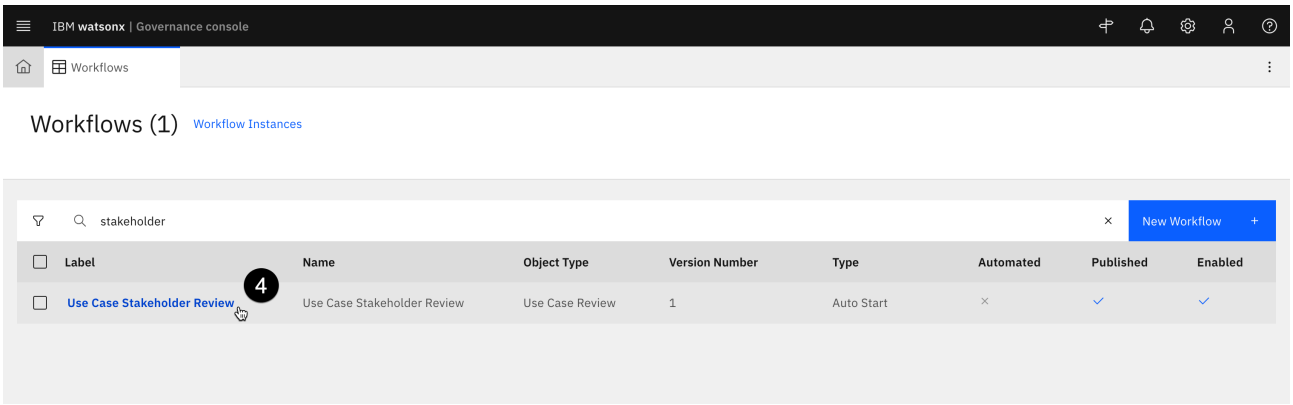
1. From the watsonx governance console, click the gear icon in the upper right to open the Administration window.

2. Click on the Solution Configuration menu item to expand it.

3. Click on the Workflows menu item. A new tab listing all the existing workflows opens. Note that you may receive a warning message about not having access to all of the items in the workflow; this can be ignored.



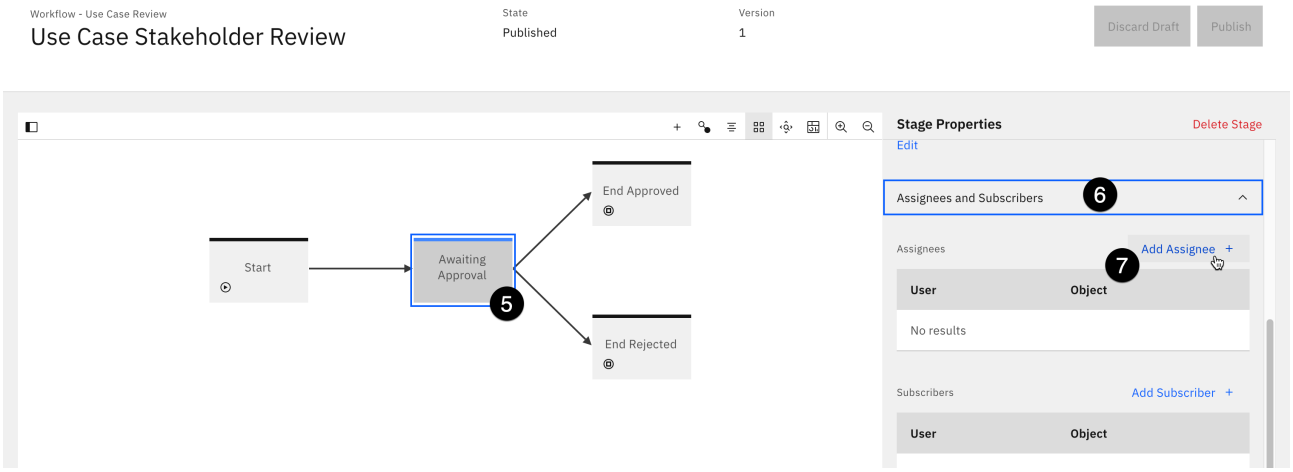
4. Locate and click on the Use Case Stakeholder Review link from the table. The workflow editor opens.



5. Click on the Awaiting Approval stage of the workflow. The Stage Properties panel opens on the right side of the screen.

6. Scroll to the bottom of the panel and click on the Assignees and Subscribers item to expand it.

7. Click on the Add Assignee button. The Assignees panel opens.

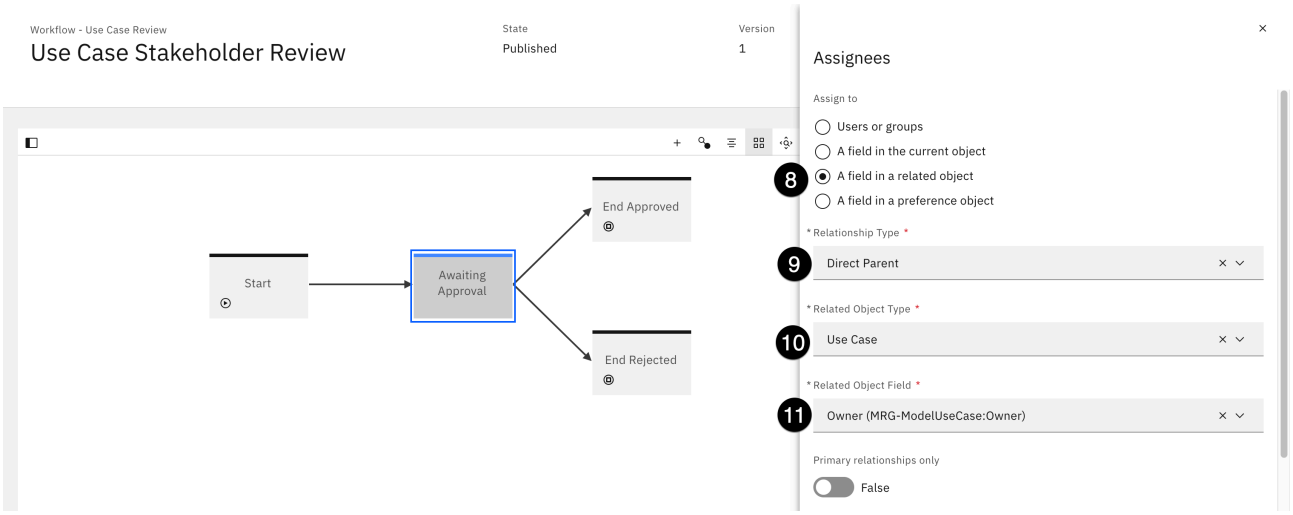


8. Click on the A field in a related object item to select it.

9. Click on the Relationship Type dropdown and select Direct Parent.

10. Click on the Related Object Type dropdown and select Use Case.

11. Click on the Related Object Field dropdown and select Owner (MRG-ModelUseCaseOwner).



12. Click the Done button to close the Assignees panel.

13. Click the Publish button to publish the changes to the workflow.

At this point in the lab, you have performed several customizations of the governance console. You have worked with user profiles, created business entities, set up custom fields, added those fields to views, experimented with questionnaires, and altered use case workflows.

The depth and configurability of the governance console is one of the major differentiators for watsonx.governance, and a successful proof of experience (PoX) should spend time highlighting these capabilities and encouraging the client to perform their own customizations based on their organization's requirements.

From this point on, the lab will focus on governing models using the workflows and processes you created and customized in the previous steps.

Choose a lab to focus on

The next two sections of the lab cover the governance of generative AI models and predictive machine learning models. You do not need to complete them in order; if your clients are more interested in predictive machine learning models, you can skip directly to that section and return to the generative AI section if you have time.

For these portions of the lab, you will continue to be signed in as the admin user for the sake of simplicity. Many of the actions that you will perform, such as configuring monitors, would be performed by platform administrators in a real-world situation. Other tasks, such as creating use case requests, would fall to business stakeholders. The user personas will be called out as you complete steps in the lab. Keep that separation in mind as you progress.

Govern generative models

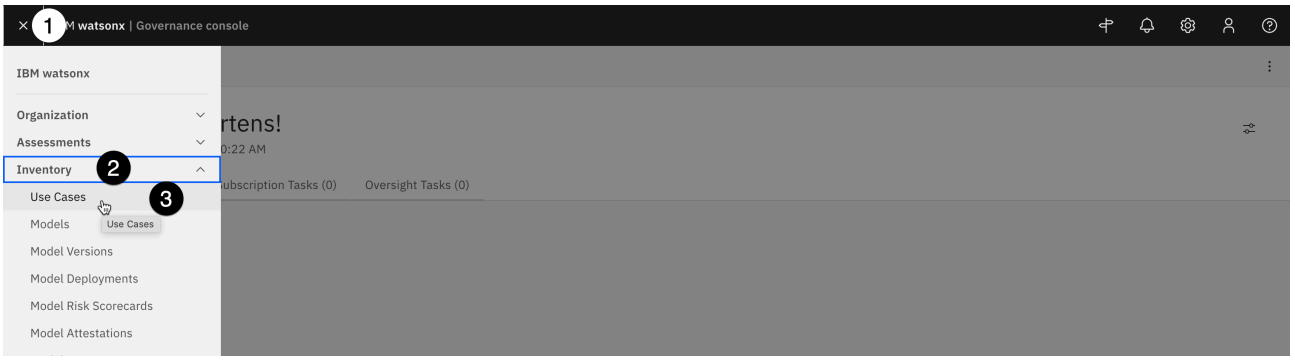
In this section of the lab, you will go through the steps of the approval workflow you customized during the governance console configuration steps. The human resources department has received a large number of applications for open positions, and would like to use AI to summarize them to help save time for the hiring department, and process the applications more efficiently to improve the experience for the applicants.

Most use cases for generative models involve interacting with prompts and prompt templates, which help users provide clear input to a Large Language Model (LLM) by giving them a structured framework to follow, which in turn helps the model generate accurate responses.

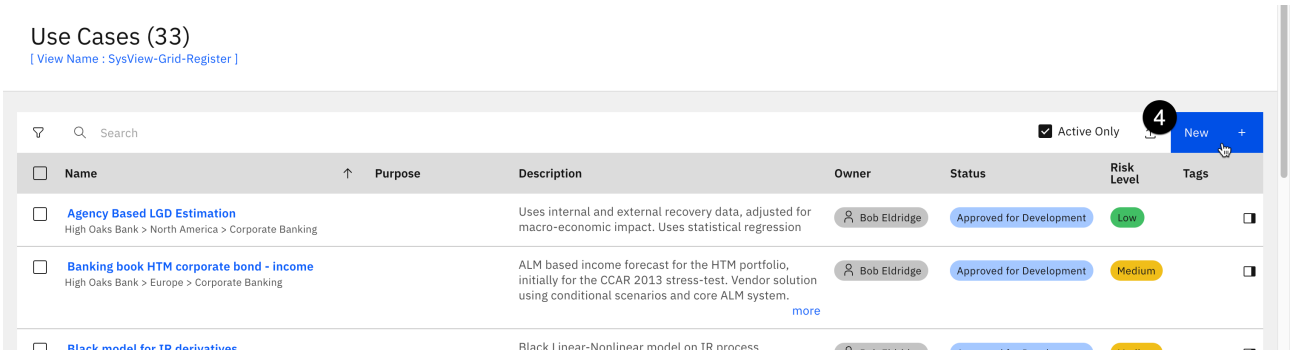
1. Create a model use case

In the day 1 lab you created a sample use case and tracked the request through the approval process, including the risk and applicability assessment questionnaires. For this lab, you will once again create a use case request, but will skip several of the steps you completed previously.

1. Click on the hamburger menu in the upper left.
2. Click on the Inventory menu item to expand it.
3. Click on the Use Cases menu item. The Use Cases tab opens. Note that several sample uses cases were loaded by the lab administrator.



4. Click the blue New button. The New Use Case tab opens.



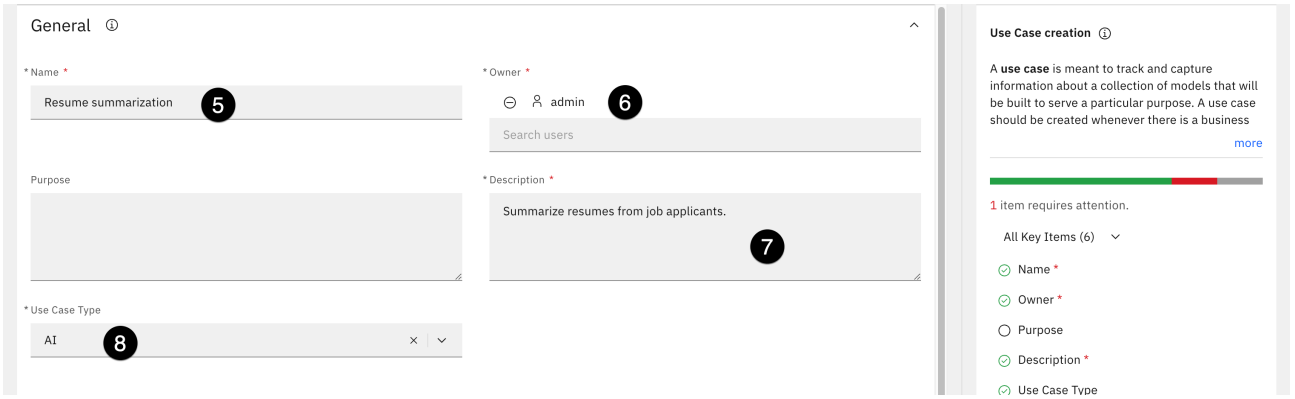
Note that the Model Use Case creation information panel on the right of the screen offers helpful information about model use cases, as well as a list of required fields. Clicking on any of the fields in that panel will scroll the screen directly to that portion of the form, helping you quickly rectify any items needing attention.

5. In the General section of the form, enter Resume summarization in the Name field. Note that when you enter a value in the field, the progress bar in the Model Use Case creation information panel updates.

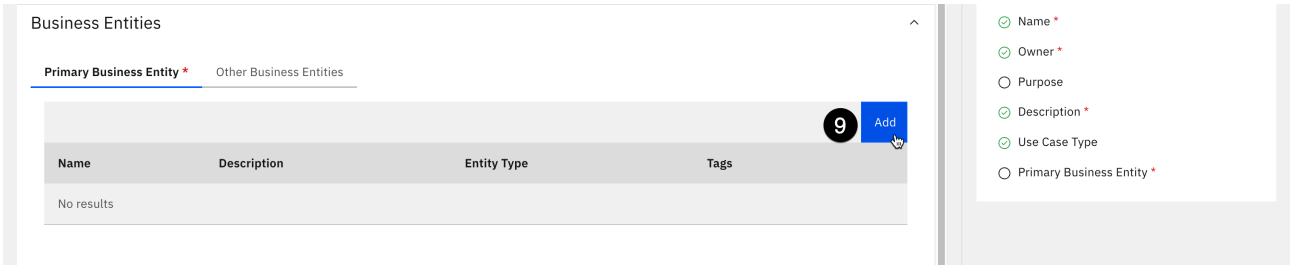
6. Click the Owner field and enter the admin user into this field. DO NOT select any of the sample users that were loaded during the system configuration import step, as they will not have associated Cloud Pak for Data accounts and will not be able to log in and work with the use case.

7. Enter a description in the Description field.

8. Click on the Use Case Type dropdown and select AI.

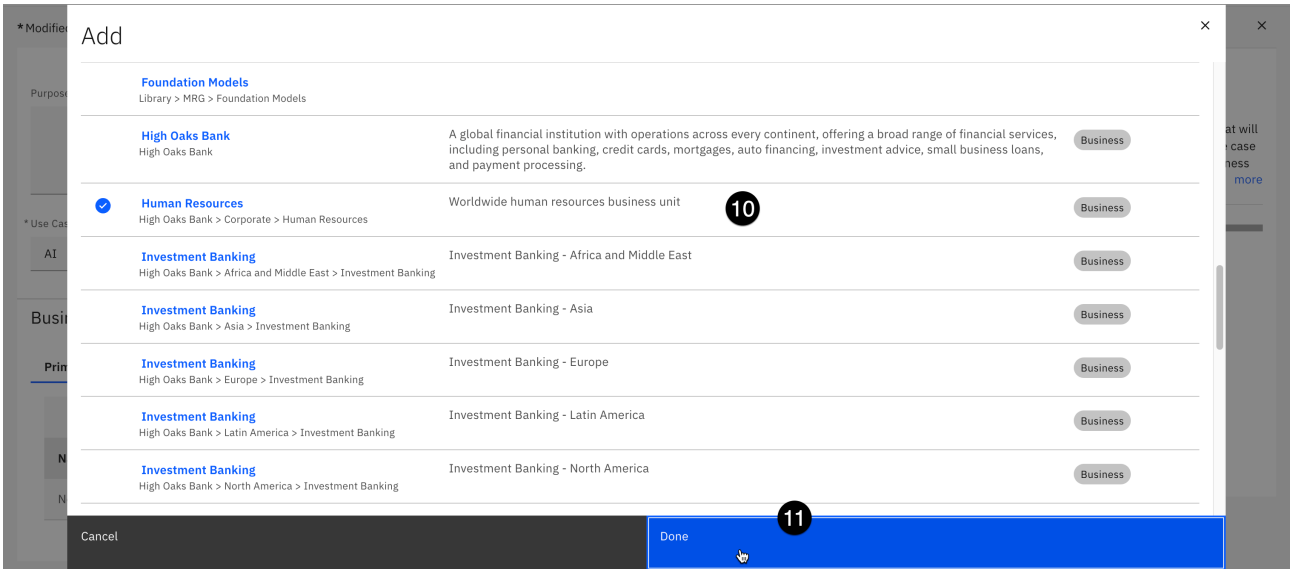


9. All model use cases are owned by business entities, representing the part of the organization responsible for requesting the use case. In the Business Entities section of the form, click the Add button. The Add window opens with a list of business entities defined for the organization.



10. Locate the Human Resources entity from the list and click on it to select it.

11. Click Done to add the business entity to the use case. The Add window closes.



12. Click the Save button in the upper right to save the use case.

When the use case has finished saving, the screen will reload with the view you customized in previous steps; you should see the Secondary EU AI Review field in the Regulatory Information section of the use case. At this point, the use case has been created and is now governed by the Use Case Request workflow that you modified. Specifically, it is in the Use Case Data Gathering stage of the workflow.

To progress the use case through the workflow, you will now need to perform the actions specified in the Action items in the workflow.

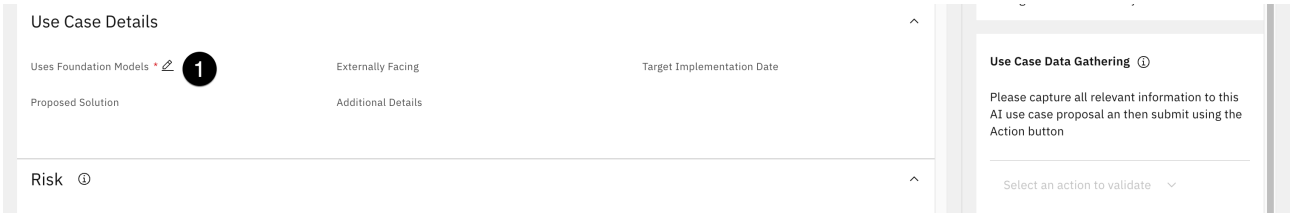
2. Progress the use case to the next phase

The use case request has progressed to the data gathering stage of the workflow, and has been assigned as an action for the appropriate owner. Recall that owners of each stage of the workflow can be configured, and alerts assigned.

In the day 1 lab you progressed a use case through the approval process, filling out the risk assessment questionnaire to identify possible risks. For the sake of time, in this lab you will use your administrator's authority to manually attach risks to the use case and then advance it to the proper lifecycle phase.

In an earlier section of the lab, you updated the model use case review to hold a new field (Secondary EU AI Review). When performing a PoX for your client, you may wish to add other fields to this view, which may contain other required information to be filled out in this stage. Information could include things like billing codes, additional documentation or justification, or more. In this case, you will only edit required fields specified in the information panel on the right before progressing to the next stage of the workflow.

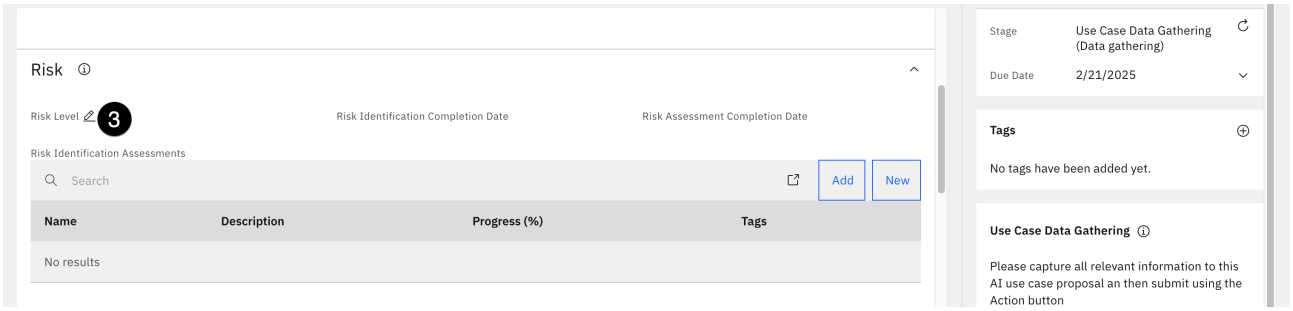
1. Scroll to the Use Case Details section of the view and click on the pencil icon that appears when you hover your mouse over the Uses Foundation Models field.



2. Use the dropdown to set the field to Yes.

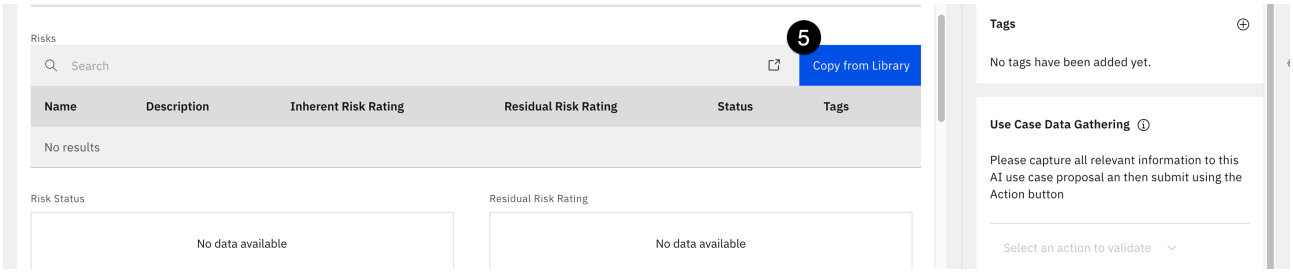
Risk Level represents the risk to the organization should issues arise with the models used to address the requirements laid out by the use case. A full risk assessment is beyond the scope of this lab; however, because hiring and employment violations can lead to expensive litigation damage to an organization's reputation, this use case will be marked as high risk.

3. In the Risk section of the form, click on the pencil icon next to the Risk Level field to edit it.



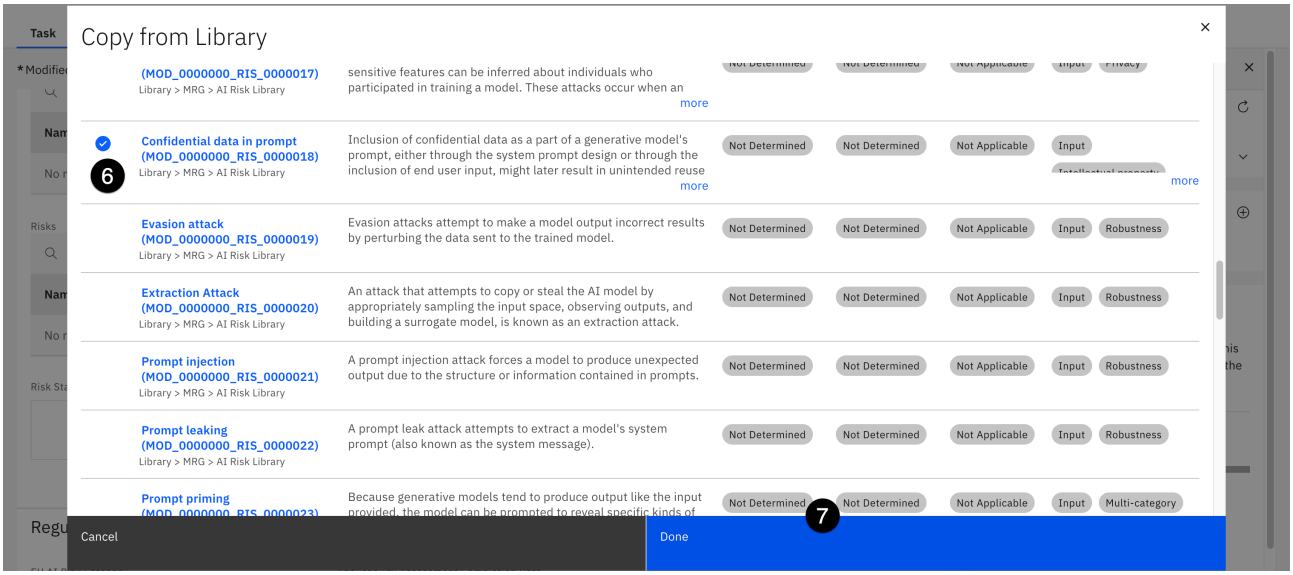
4. Select High from the dropdown.

5. Scroll down to the Risks table in the same section and click on the Copy from Library button. The Copy from Library dialog window opens, listing all the available risks currently in the library.



6. Scroll down to the Confidential data in prompt risk and click on it to select it.

7. Click on the Done button to add this risk to your use case.

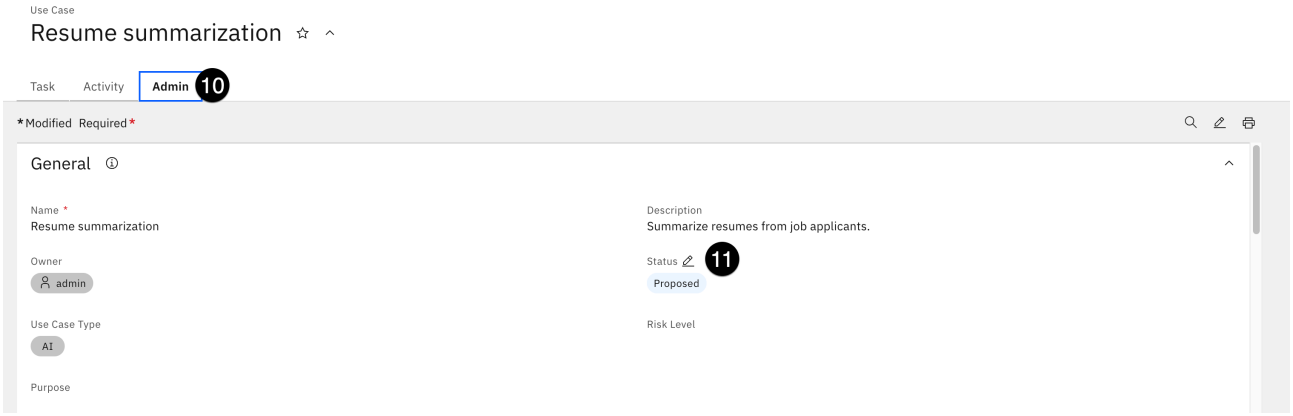


8. Repeat steps 5-7 for any other risks you wish to attach to your use case.

9. Click on the Save button in the upper right to save your use case. Note that if you see an error message saying that the use case has recently been updated by another user, you may need to refresh the page and verify that they information added to the form in previous steps has been saved, then click on the Save button again.

10. From the top of the view, click on the Admin tab.

11. Click on the pencil icon that appears when you hover your mouse over the Status field in the General section.



12. Use the dropdown to set the Status field to Approved for Development.

13. Click on the Save button to save your changes.

14. Click on the Task tab to return to the Task view of the use case.

Although you skipped many of the steps you performed in the day 1 lab, at this point in the lifecycle, the model use case has been created, reviewed for risks, and approved by the various stakeholders. Personas involved in these steps would be mostly non-technical, from the business user who requested the model to the risk and compliance officer who evaluated it. Next, the model would be developed by teams of data scientists and AI engineers. The following steps of the lab will take actions from the point of view of those personas.

3. Create the prompt template

In this case, the AI engineers have elected to work with the Azure OpenAI service on a prompt template to summarize the resumes.

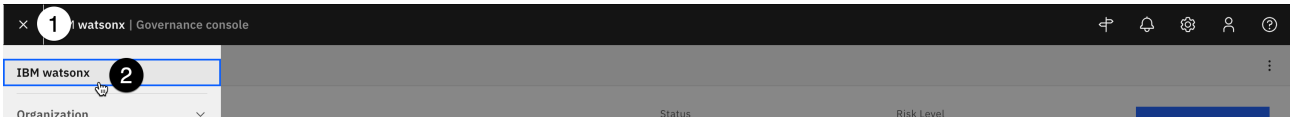
THESE EVALUATIONS ARE NOT INTENDED TO SHOW THE RELATIVE STRENGTHS OF THE OPENAI OR AZURE PLATFORMS, AND SHOULD NOT BE PRESENTED AS SUCH. The prompt used in this lab is fairly simple, and in a real-world scenario would be tuned and optimized for the individual use case. The evaluations here are presented to show how the watsonx.governance platform can collect facts and metrics for hybrid environments with models deployed on any platform.

Watsonx.governance supports the evaluation of third-party generative models via a method known as detached prompt templates, which are generative AI models not hosted on the same platform as the watsonx.governance service. At the time of writing, working with detached prompt templates is done through the use of Jupyter notebooks.

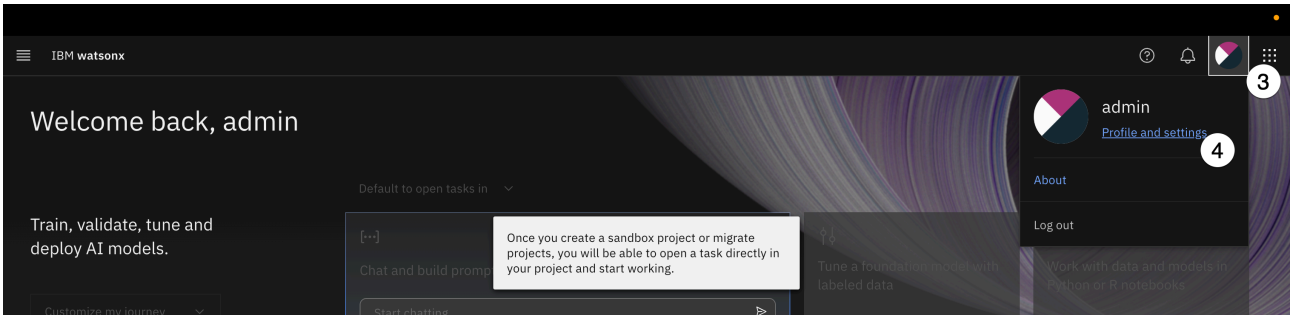
To begin, you will need to gather credentials used by the notebook. From watsonx, you will need the base Cloud Pak for Data URL, as well as the username and password of the created user. You will also create an API key for the user.

For Azure, you will need the API Endpoint, API key, name of the deployed model, Client ID, and Client Secret. Your lab instructor will provide these credentials for you.

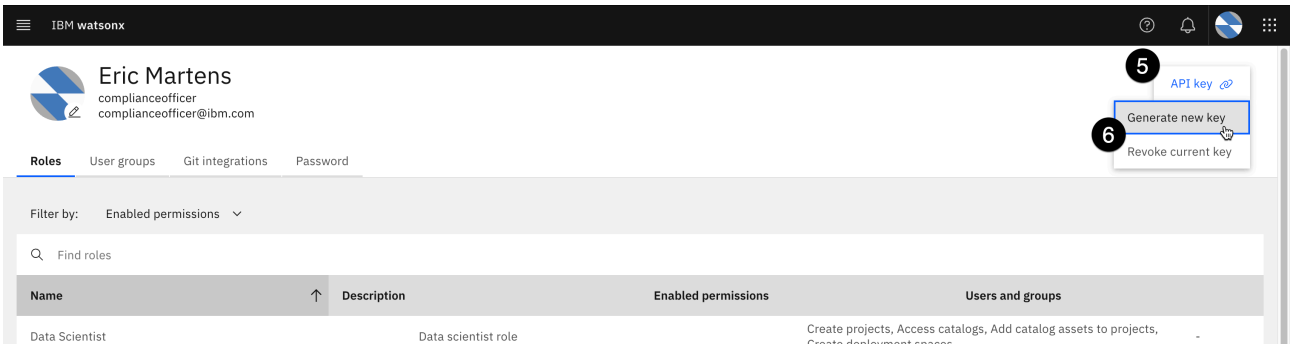
1. From the watsonx governance console, click on the hamburger menu in the upper left.
2. Click on the IBM watsonx menu item. The watsonx home page opens in the watsonx context (as opposed to the Cloud Pak for Data context).



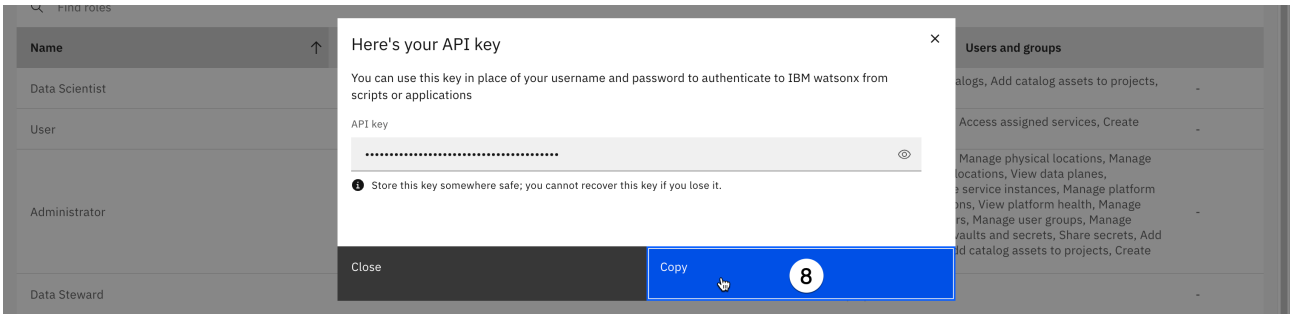
3. Click on the avatar icon in the upper right to open the user menu.
4. Click on the Profile and settings item from the menu. The user profile screen opens.



5. Click on the API key button in the upper right. The API key menu opens.
6. Click on the Generate new key menu item. The Generate new API key? dialog window opens.



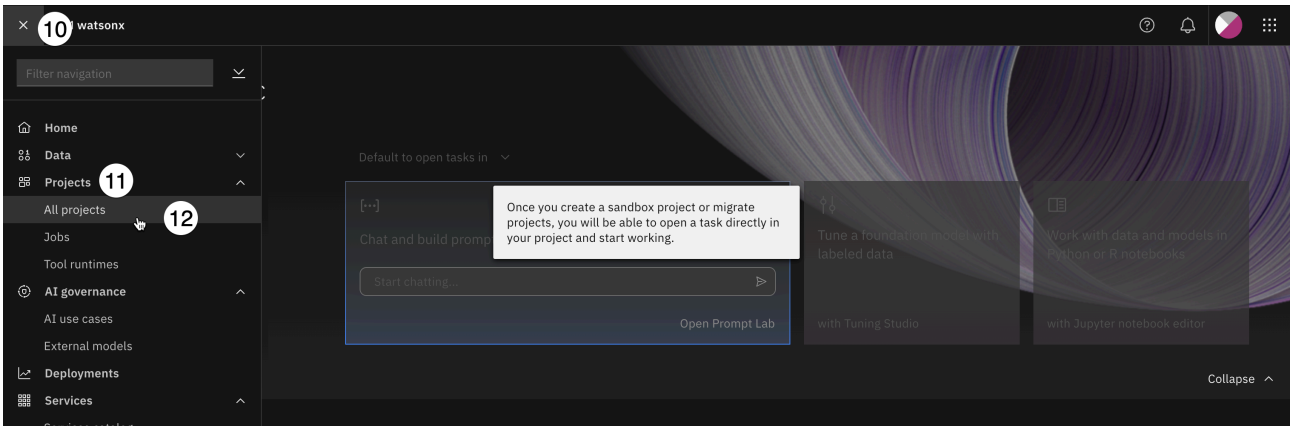
7. Click the red Generate button to confirm API key creation. Note that, as the warning states, generating a new key will invalidate any existing keys you have.
8. Click the Copy button to copy your new key to the clipboard. Paste it into a text file for later use in the notebook, where it will represent the CPD_API_KEY value.



9. Once you have pasted the key into a text file, click the Close button to close the window.
10. Click on the hamburger menu in the upper left.

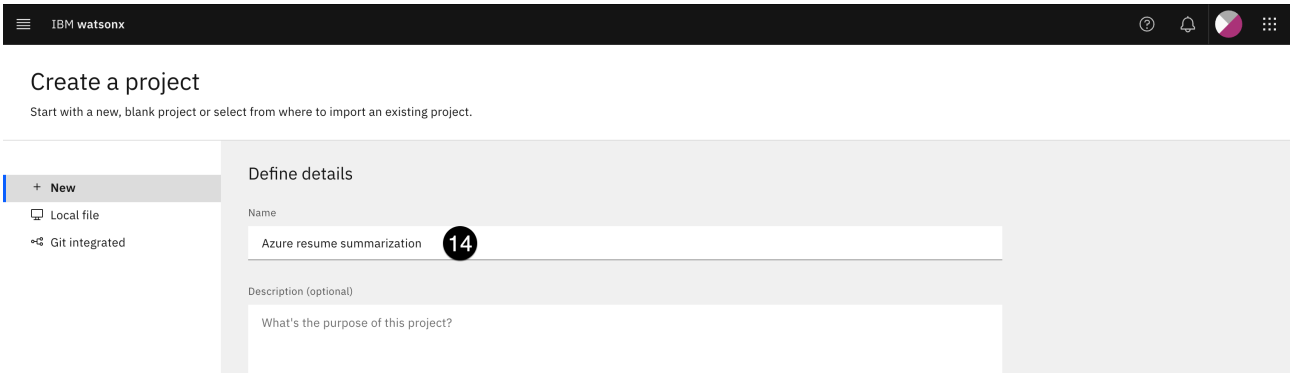
11. Click on the Projects menu item to expand it.

12. Click on the All projects menu item. The Projects screen opens.



13. Click on the New project button. The Create a project screen opens.

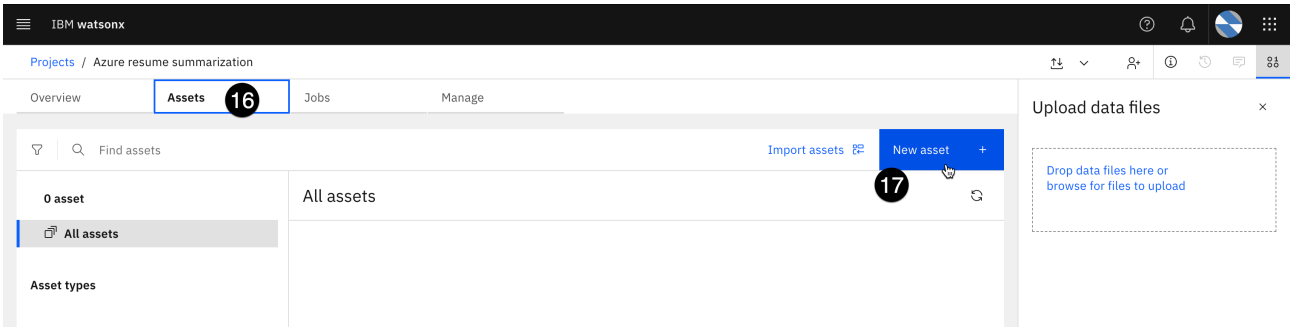
14. Give your project a Name.



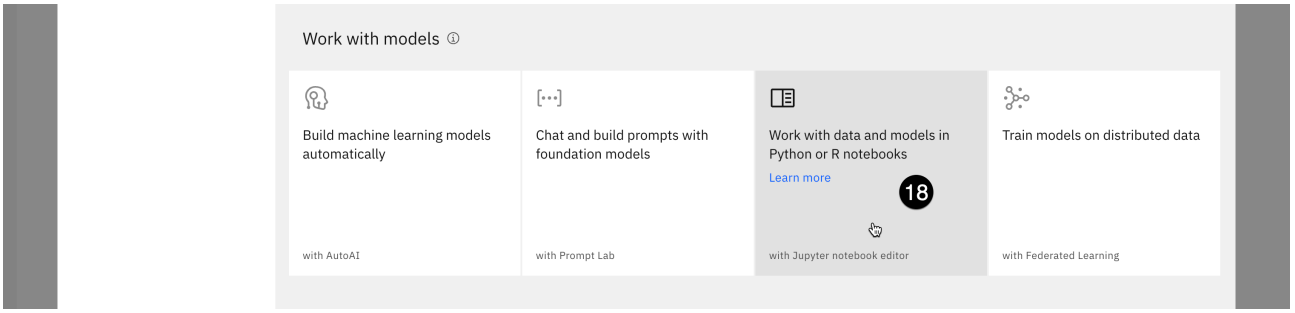
15. Click the Create button. Your project will be created.

16. Click on the Assets tab.

17. Click on the New asset button. The What do you want to do? window opens.

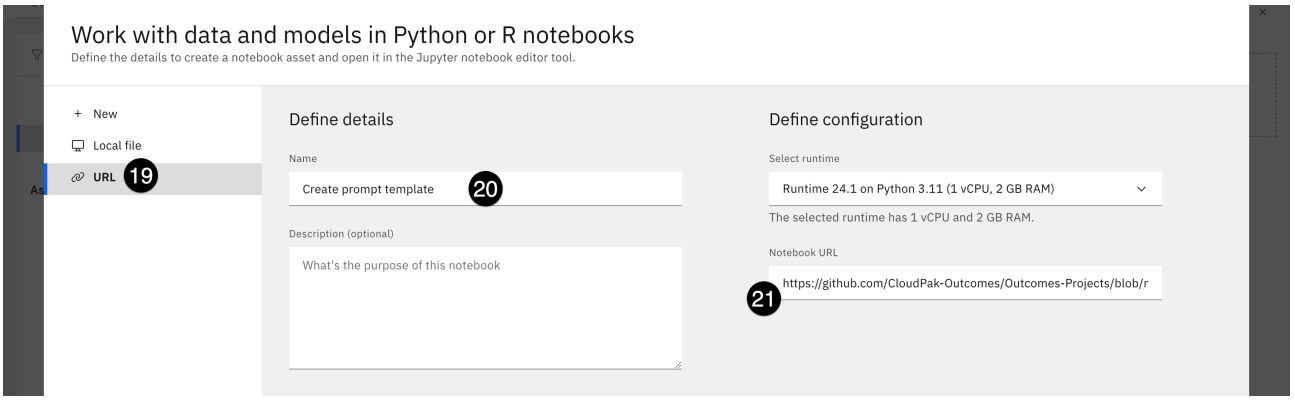


18. Locate and click on the Work with data and models in Python or R notebooks tile.



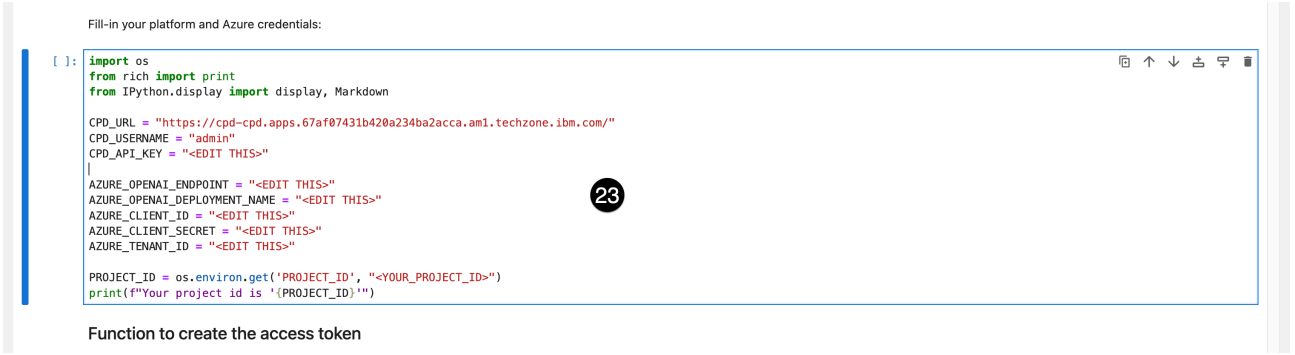
19. Click on the URL option.
20. Give your notebook a Name.
21. Copy and paste the following URL into the Notebook URL field:

```
https://github.com/CloudPak-Outcomes/Outcomes-Projects/blob/main/watsonx-governance-14-deploy/governance/create_prompt_template_51.ipynb
```



22. Click the Create button. Your notebook will be created.
23. Scroll down to the code cell that contains the platform and Azure credential variables, and edit the string values. Your CPD_USERNAME will be admin. The CPD_PASSWORD will be the administrator password for your environment. The CPD_API_KEY is the API key you generated in a previous step for the created user.

The Azure credentials will be provided by your lab instructor.

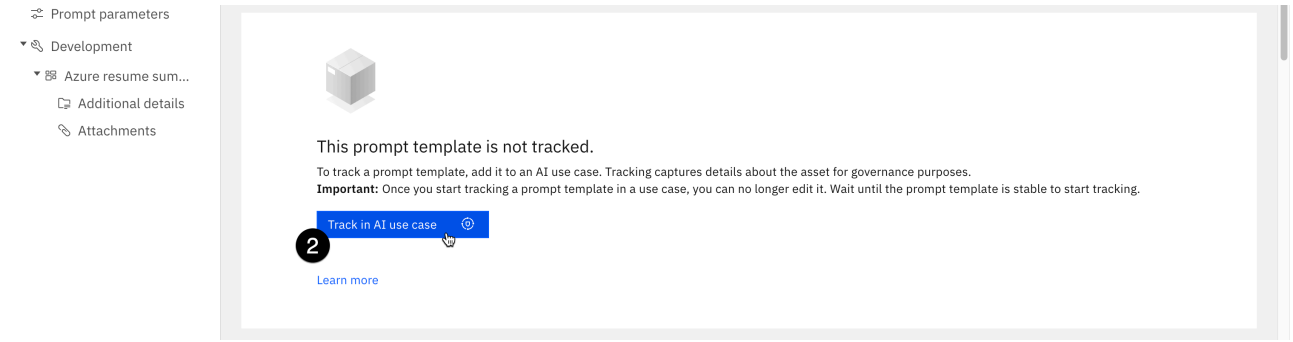


24. Run through the code cells in the notebook one at a time. The notebook will connect to the OpenAI model, use it to perform resume summarization on sample resumes, and finally save the prompt template to your project. It will also save the summaries to a CSV file in your project that you will use to evaluate the template's performance.
25. Click on the link to your project in the upper left to return to the project screen.
26. From the Assets tab on your project screen, click on the Detached prompt template... to open it.

4. Track the prompt in the use case

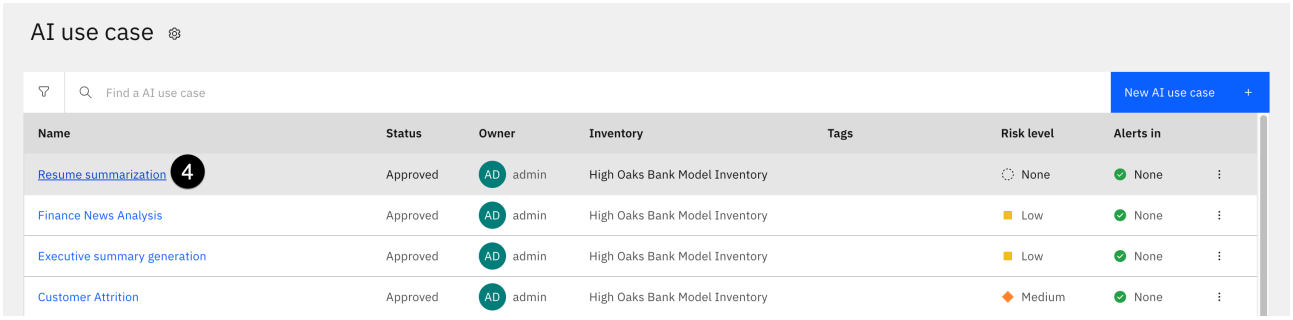
Next, you will associate the prompt template with the use case that you took through the approval process.

1. Close the Learn about your AI asset window that appears.
2. Click on the Track in AI use case button. A warning dialog appears, notifying you that your project is not associated with an AI use case.



3. Click on the Go to AI use cases button. A new browser tab opens with a table of AI use cases has been populated from the watsonx governance console, including the Resume summarization use case you created.

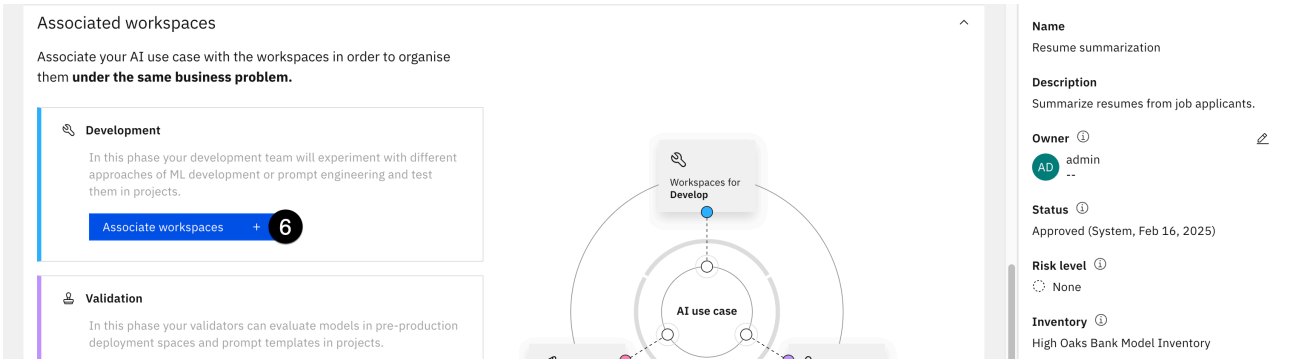
4. Click on the name of the Resume summarization use case to open the use case.



Note that this view of the use case differs from the one in the governance console. It is aimed more at model developers and AI engineers. However, the data in this view is automatically synchronized with the governance console, ensuring that all stakeholders have immediate access to the most up-to-date information.

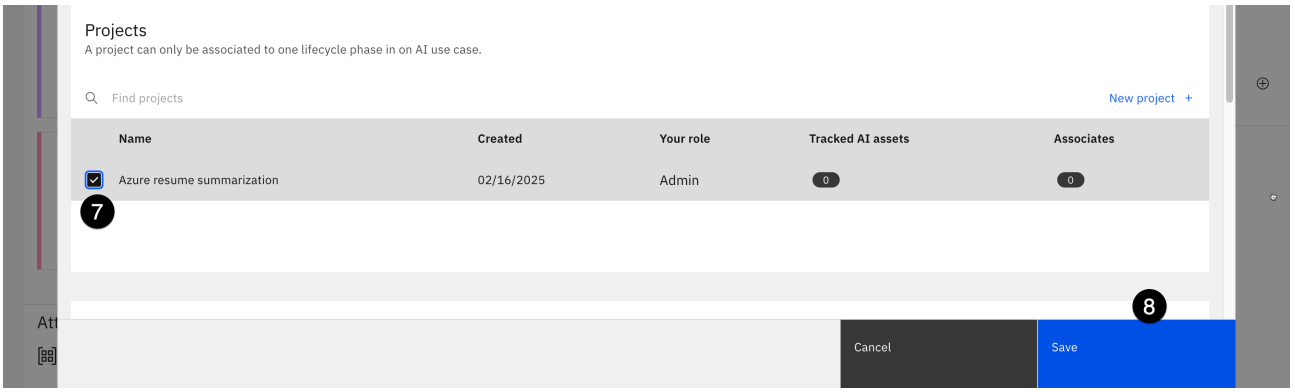
5. Scroll down to the Associated workspaces section of the use case. Note that there are three model lifecycle sections here: *Development*, *Validation*, and *Operation*. Each section can be associated with workspaces. Workspaces refer to places for data scientists, AI engineers, data engineers, subject matter experts, and others to collaborate on machine learning and AI tasks. Workspaces include projects, such as the one you created to work with the notebook, as well as deployment spaces, which are used to manage testing and production environments for models and prompts.

6. Click on the Associate workspaces button in the Development section. The Associate workspaces window opens.



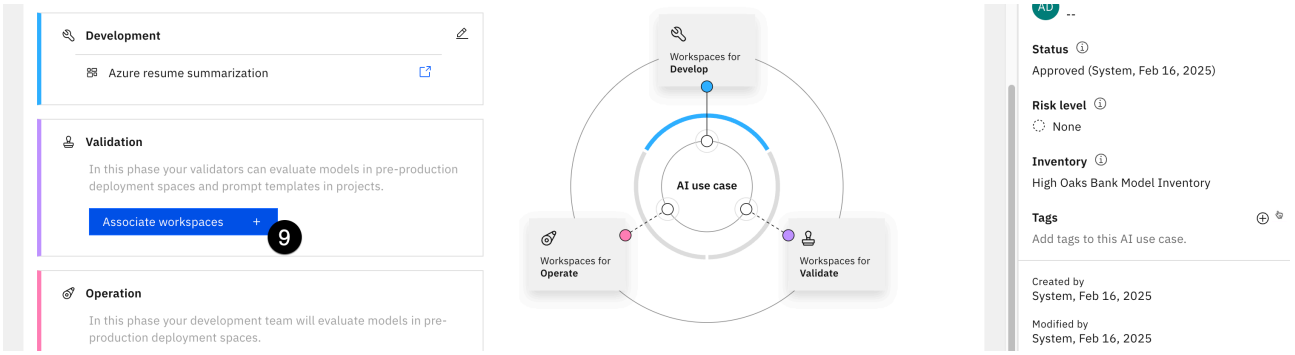
7. Scroll down to the Projects section of the window and check the box next to the Azure resume summarization project you created. This associates the project and its assets with the Development phase of the Resume summarization use case.

8. Click on the Save button to save the association. The window closes.

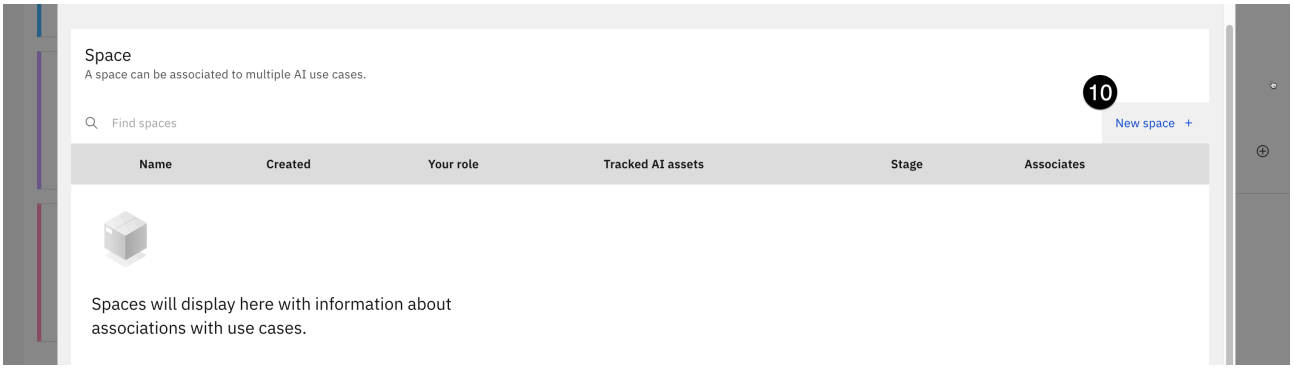


For the sake of time, at this point you will also create the deployment space for the next phase of the lifecycle, and associate it with the use case.

9. Click on the Associate workspaces button in the Validation section. The Associate workspaces window opens again.

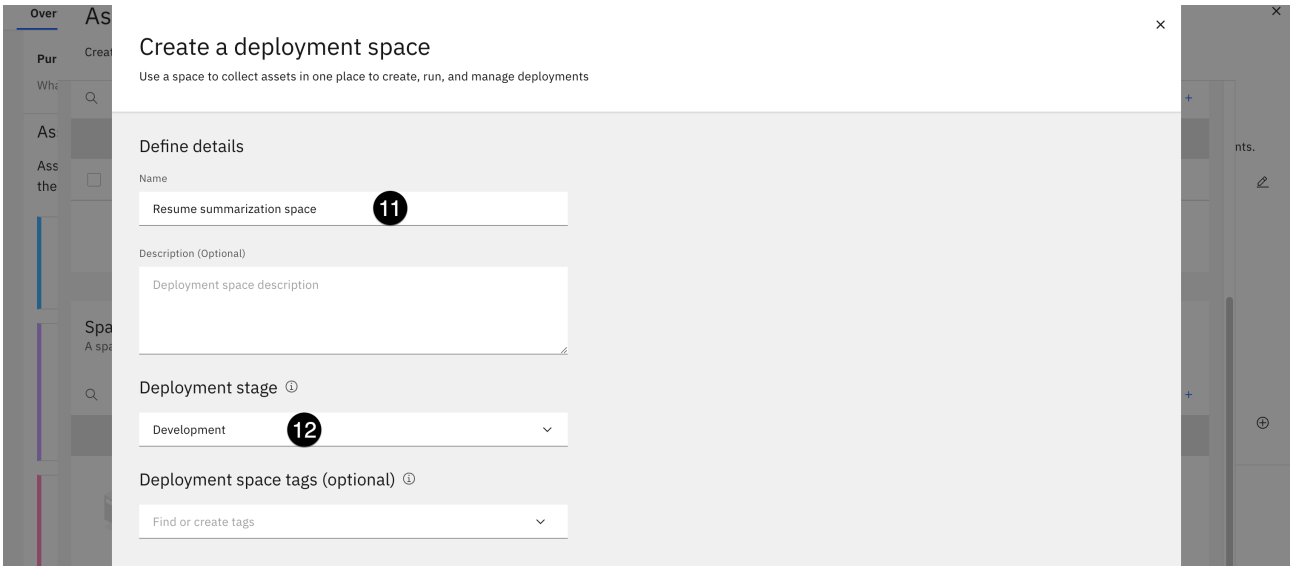


10. Scroll down to the Space section of the window and click on the New space button. The Create a deployment space window opens.



11. Give your space a Name.

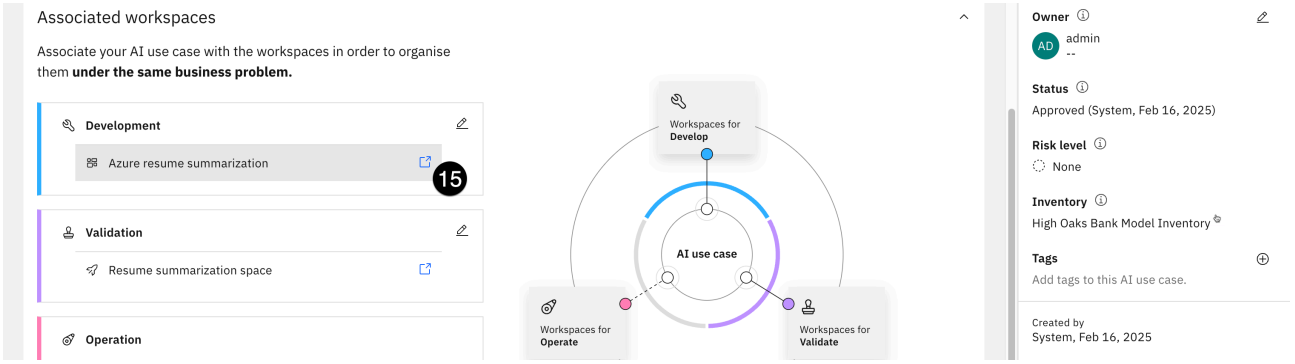
12. Click on the Deployment stage dropdown and select Development.



13. Click on the Create button to create the space. When creation is completed, close the notification window to return to the Assign workspaces window.

14. Click on the Save button to save the association and close the Associate workspaces window.

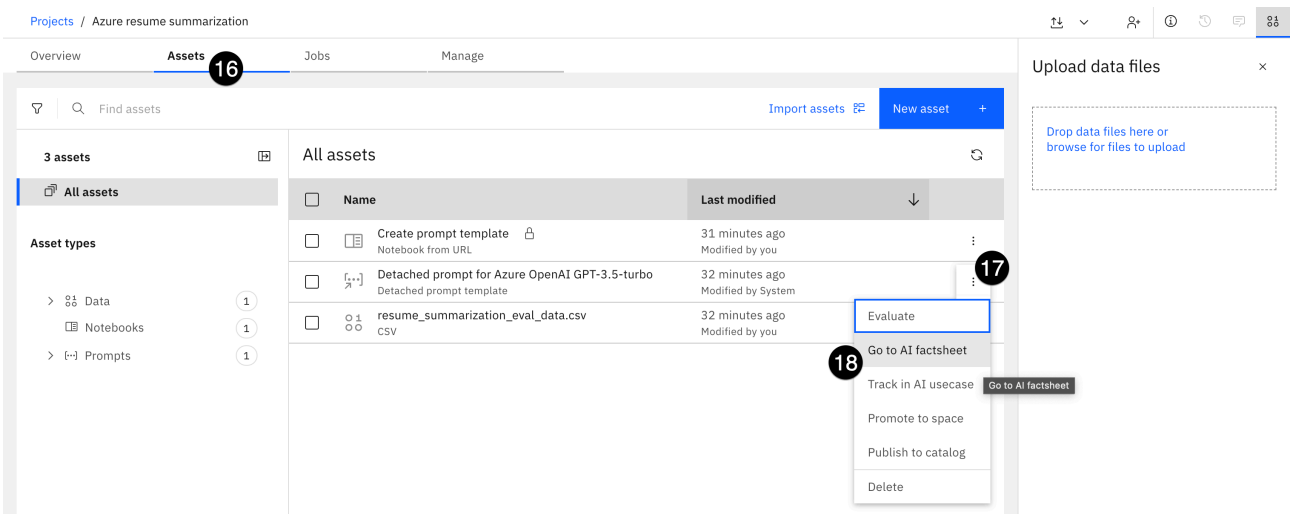
15. Return to the project by clicking on the link in the Development section of the Associated workspaces. A new browser tab opens for the project.



16. Click on the Assets tab of the project.

17. Locate the Detached prompt for Azure... asset from the table, and click on the three vertical dots to open the context menu.

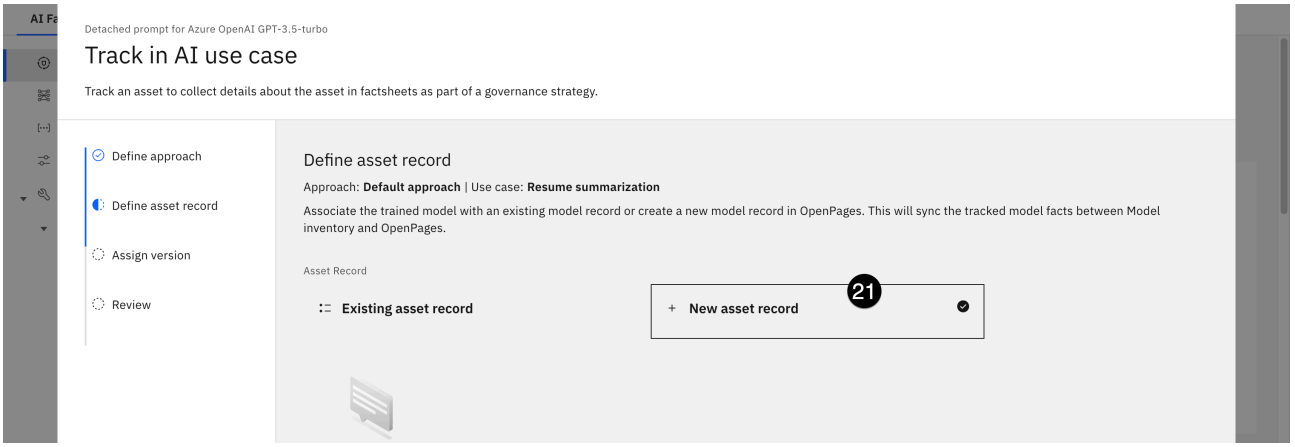
18. Click on the Go to AI factsheet menu item. A new browser tab with the factsheet opens.



19. Click on the Track in AI use case button once again. The Track in AI use case window opens to the Define approach panel.

20. Click on the Next button to accept the default approach. The Define asset record screen opens.

21. Click on the New asset record tile to specify that you would like to create a new model in the governance console inventory.

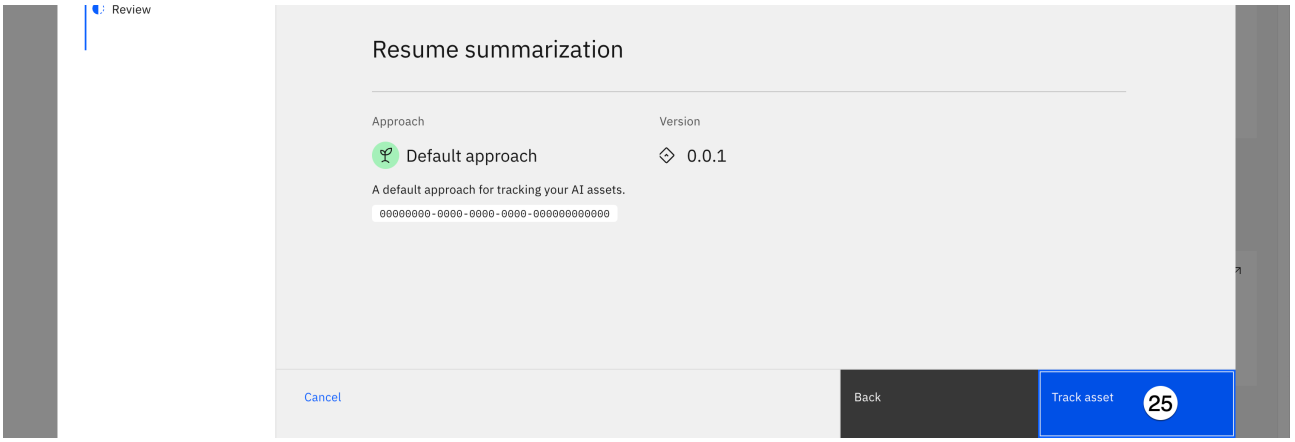


22. Click on the Next button. The Assign version screen opens. This screen allows you to set a version number for your model based on its progress in development.

23. Click on the Next button. The Review screen opens.

Note the Important warning at the top of the screen; once you begin tracking the template in an AI use case, you can no longer edit it. This limitation may seem inconvenient. However, changes to the prompt template would invalidate any metrics gathered for it, so any revisions should be treated as separate models in the inventory for tracking purposes. Remember that a use case can have multiple models and prompts associated with it, including not only the production models, but also candidate models being tested as possible replacements.

24. Click on the Track asset button to enable tracking for the model.



> Note: Occasionally, slow network conditions may result in an error message at this point telling you that the model is already being tracked. In this case, the tracking request has typically succeeded. Clicking the Cancel button to return to the Factsheet and then refreshing the page will show the model as being tracked within the use case.

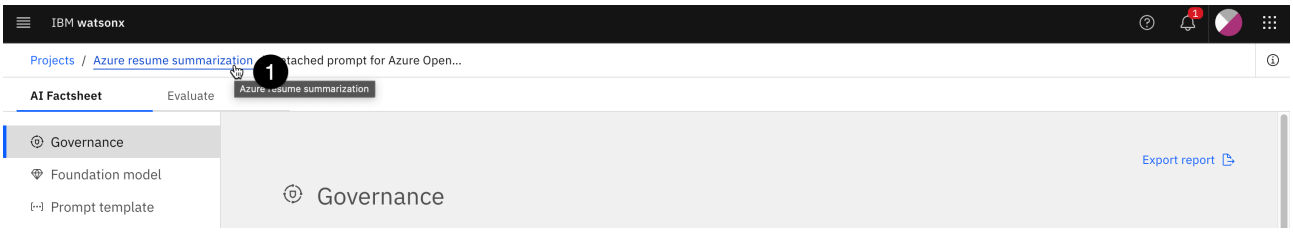
25. Take a moment to review the factsheet. Note that it contains metadata on the type of model, provider, task, and prompt.

The model has been created in the project, and is being tracked as part of a use case. Next, you will deploy the model to a space for evaluation.

5. Deploy the model to a space

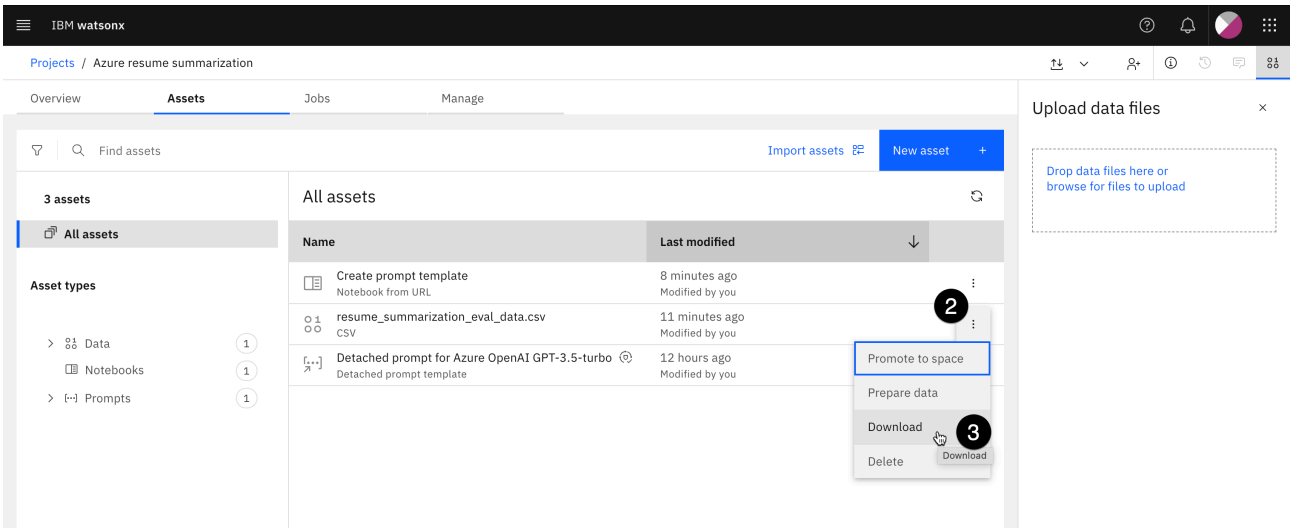
The model is now listed as an asset in your project. In this step, you will download the output to use in an evaluation, and promote the model to a space.

1. Click on your project name from the breadcrumb trail at the top of the Factsheet. The project screen opens.



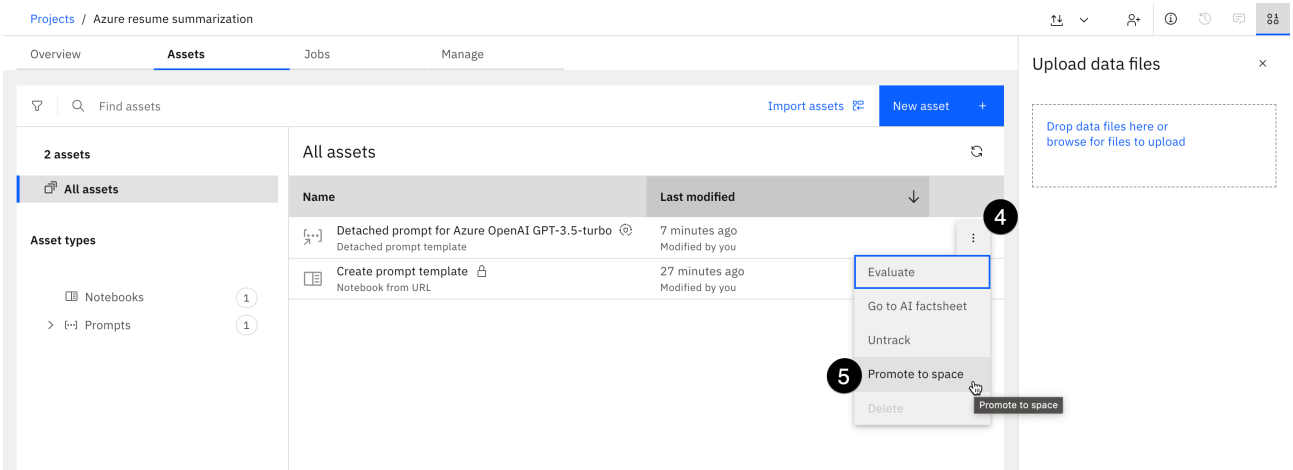
2. From the Assets tab, click on the three vertical dots to the right of the resume_summarization_eval_data.csv file to open the context menu.

3. Click on the Download menu item to download the file to your machine.



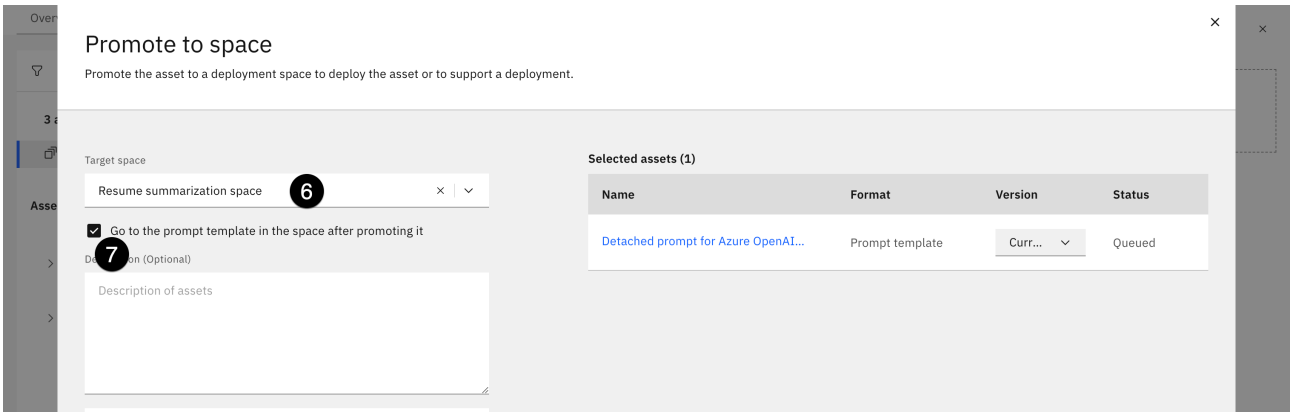
4. From the Assets tab, click on the three vertical dots to the right of the Detached prompt template... to open the context menu.

5. Click on the Promote to space menu item. The Promote to space window opens.



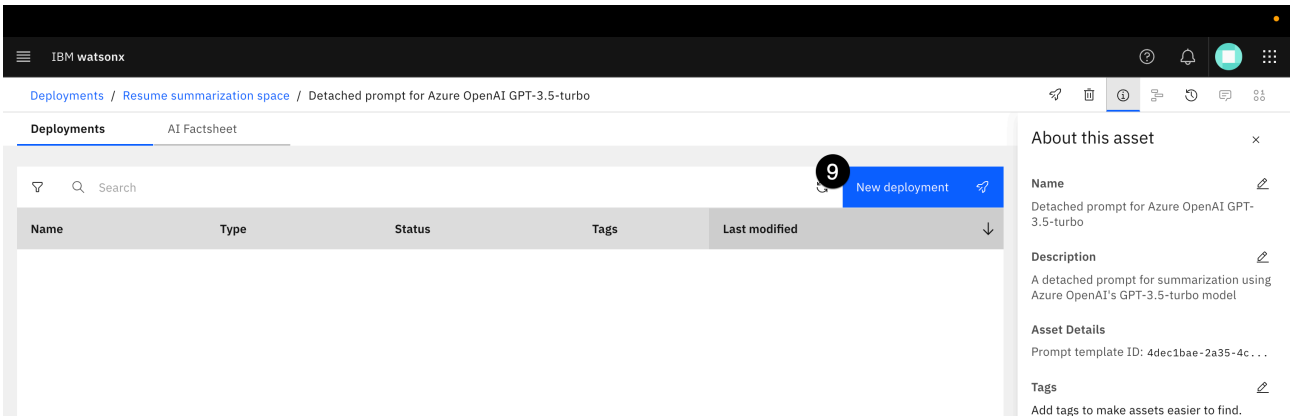
6. Click on the Target space dropdown and select the deployment space you created in a previous step.

7. Check the box to the left of Go to the space after promoting the assets.

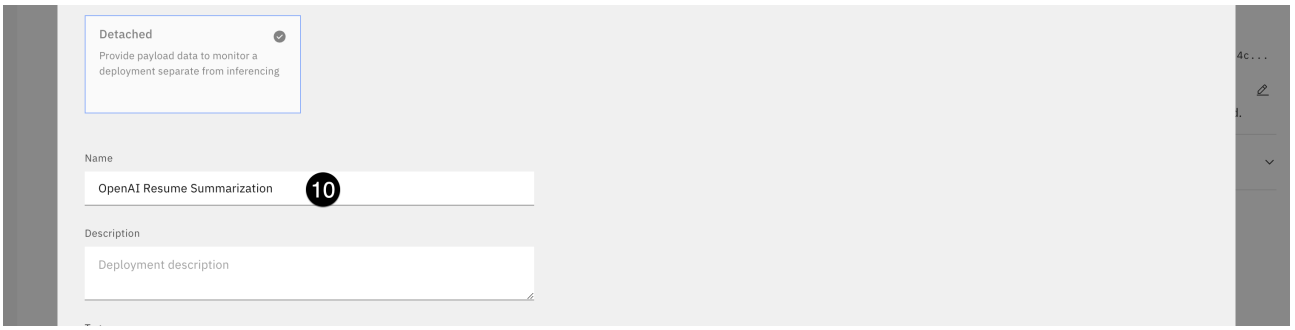


8. Click on the Promote button to promote the model. The model will be created in the new space, and the deployment space screen opens.

9. Click on the New deployment button. The Create a deployment screen opens.



10. Give your deployment a Name.



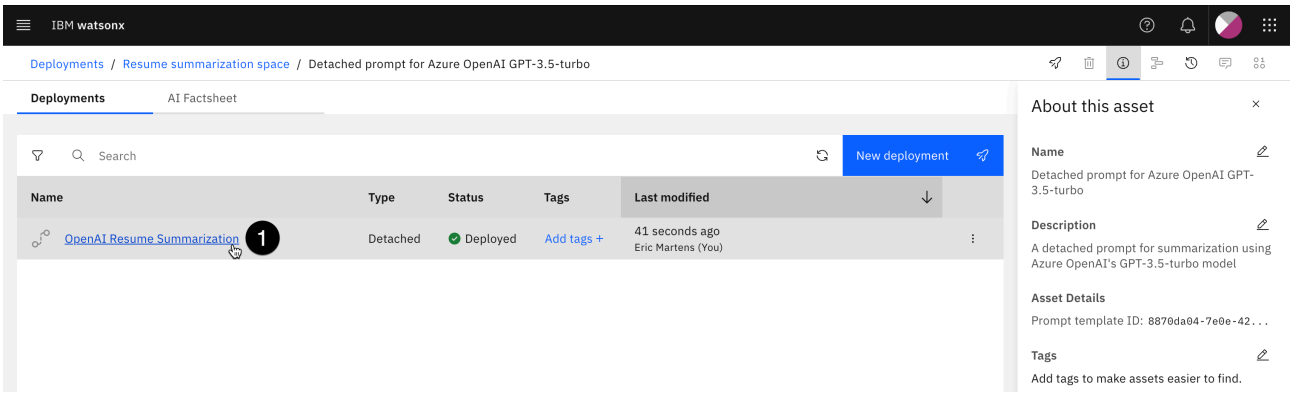
11. Click on the Create button to create the deployment.

The prompt is now available as a REST endpoint. It can also be evaluated.

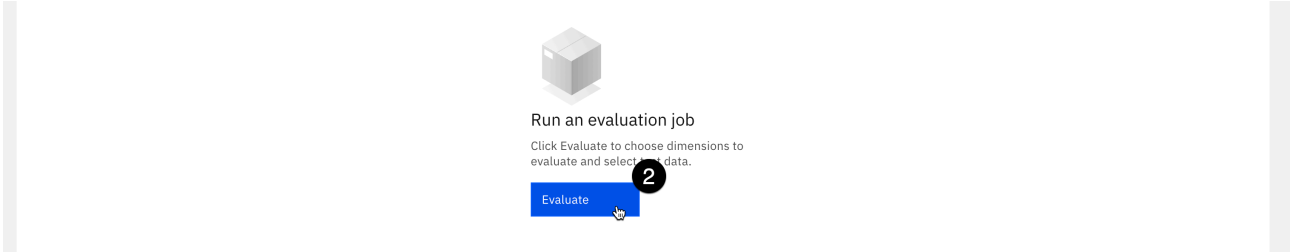
6. Evaluate the model

In this step, you will evaluate the model for quality.

1. Click on the link for your newly-created deployment. The deployment summary screen opens.

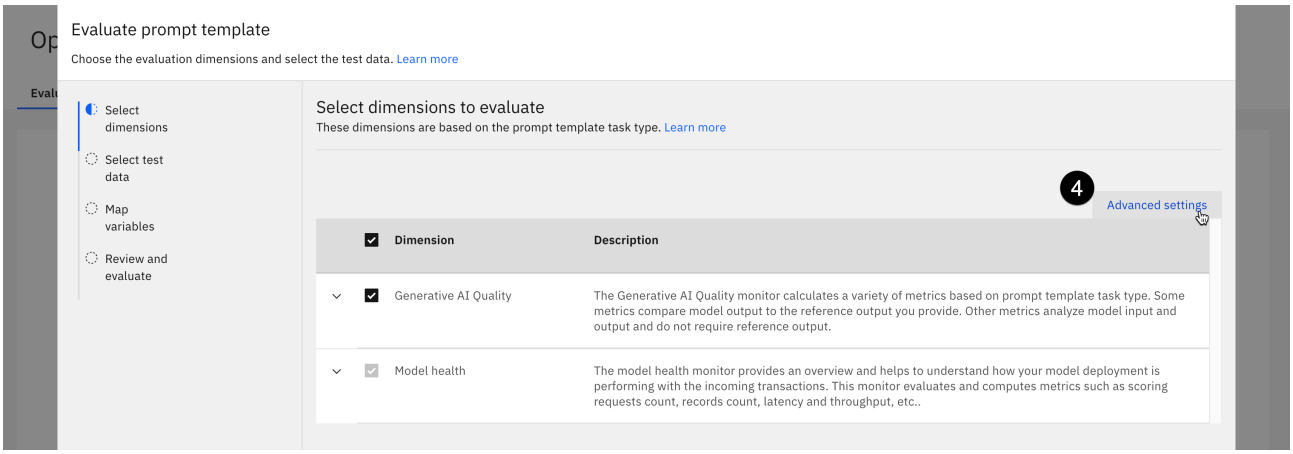


2. From the Evaluations tab, click on the Evaluate button. The Associate a service instance popup appears.



3. Click on the Associate a service instance button to associate a machine learning service with the space. The Evaluate a prompt template window opens. By default, the prompt will be evaluated for generative AI quality and model health. However, you can configure the acceptable thresholds for these metrics.

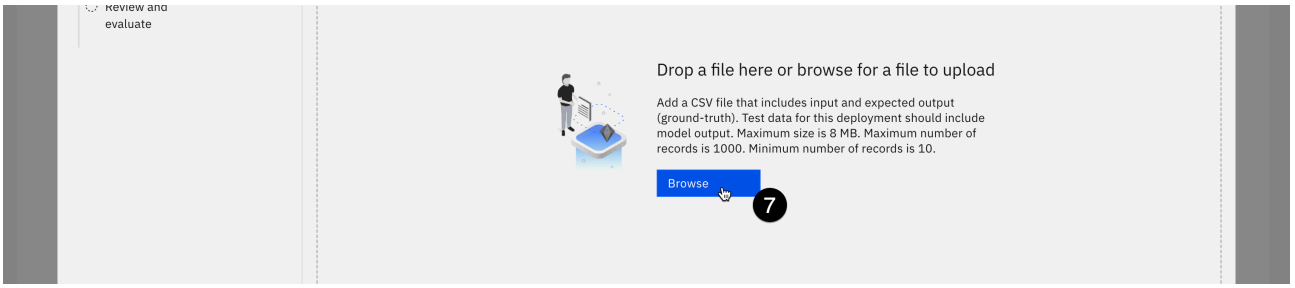
4. Click on the Advanced settings button. The configuration window for the evaluation metrics opens.



5. Take a moment to review the different thresholds for quality and model health on this screen. The model will be evaluated on metrics including ROUGE, SARI, METEOR, and others. The thresholds have been pre-set to reflect industry standards for acceptability in these metrics. However, they can be customized to meet any specific thresholds set forth by government or industry regulations in the region in which the prompt will be used. When you are finished, click the Save button if you made any changes, or click the Cancel button to return to the Select dimensions to evaluate screen.

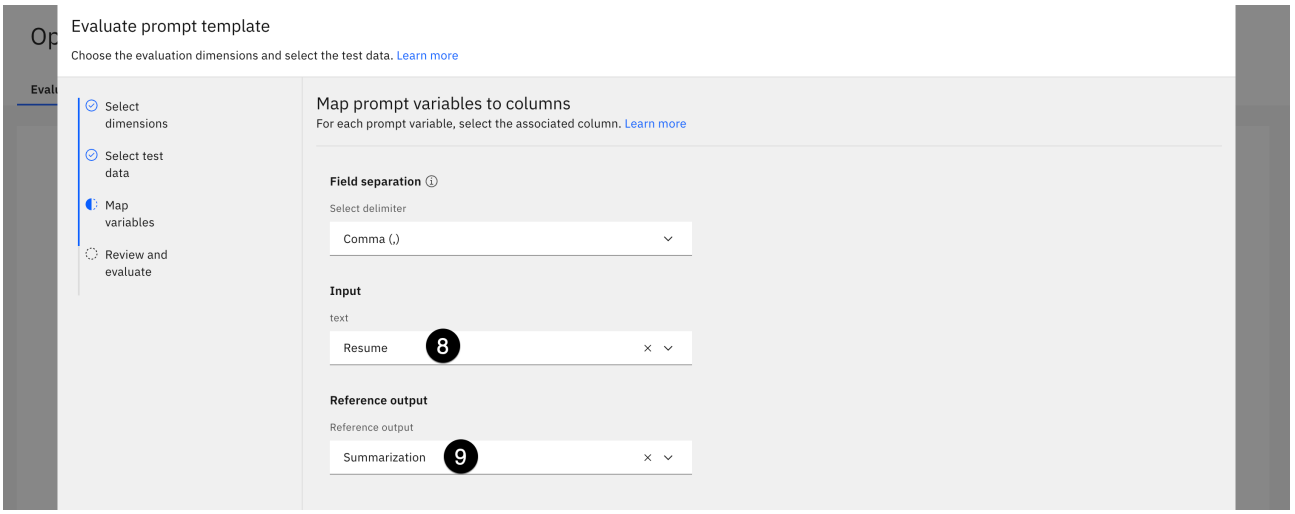
6. Click on the Next button to advance to the Select test data screen.

7. Drag and drop the *resume_summarization_eval_test_data.csv* file you downloaded from your project in the previous step into the appropriate area on the screen, or click the Browse button and browse to the file. If you were unable to generate the file, you can download a version of it from GitHub. The Map prompt variables to columns window opens when the file finishes uploading.



8. Click on the text dropdown in the Input section and select Resume.

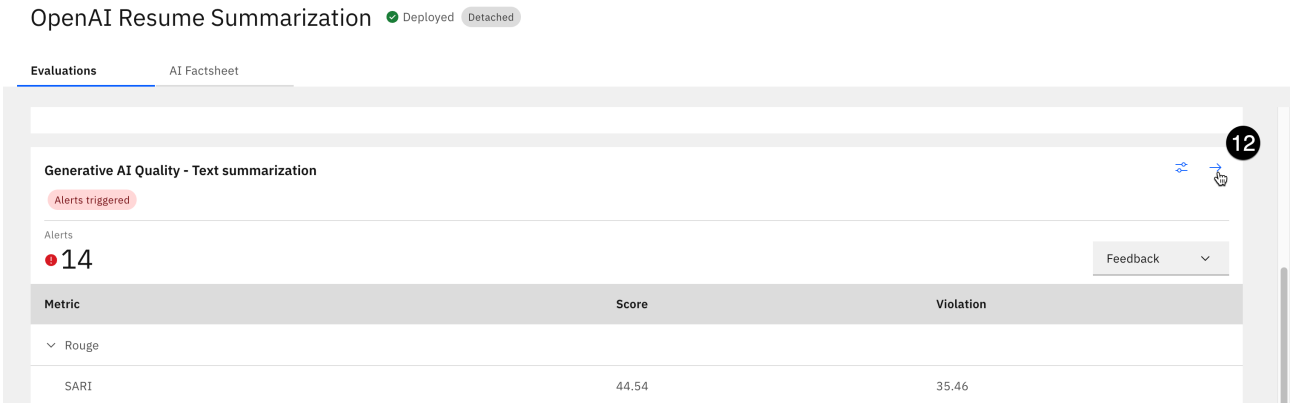
9. Click on the Reference output dropdown and select Summarization.



10. Click on the Next button. The Review window opens.

11. Click on the Evaluate button to run the evaluation, which can take several minutes to complete. Note that the evaluation may fail due to slow network conditions. These failures can frequently be fixed by re-running the evaluation with the same file.

12. Click on the arrow icon to open an expanded view of the metrics.



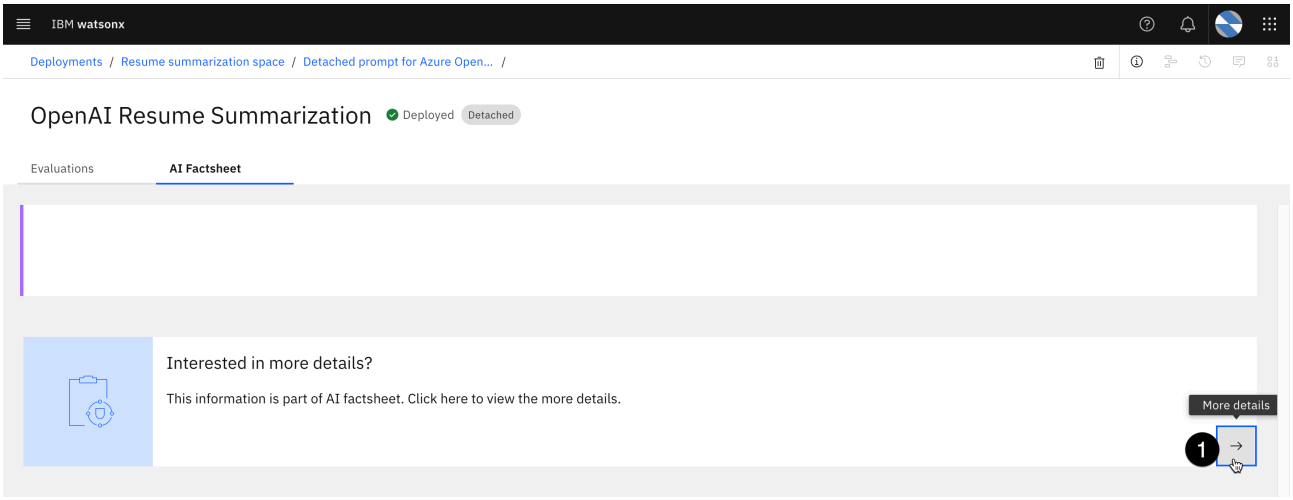
13. Take a moment to review the metrics that have been calculated. For more information on the individual metrics, see the watsonx.governance documentation.

14. Click on the AI Factsheet tab, and note that the model's Factsheet now contains the model's metadata as well as the evaluation results.

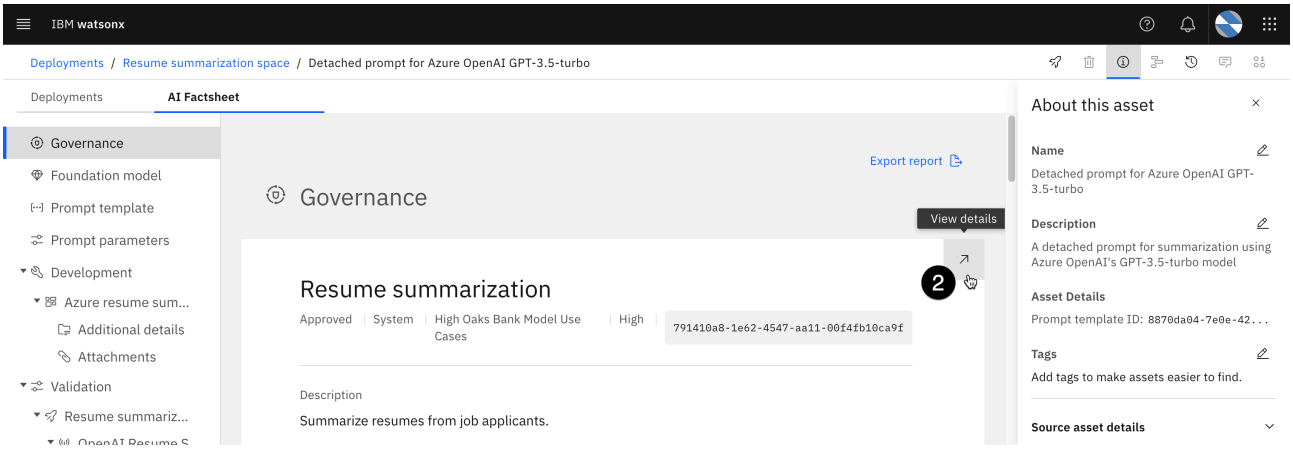
7. View the metrics in the governance console

Now that the metrics have been calculated, they can be viewed in the governance console. The watsonx service automatically updates the model's records in the governance console with the metrics information, allowing stakeholders to be sure that they are viewing the latest data.

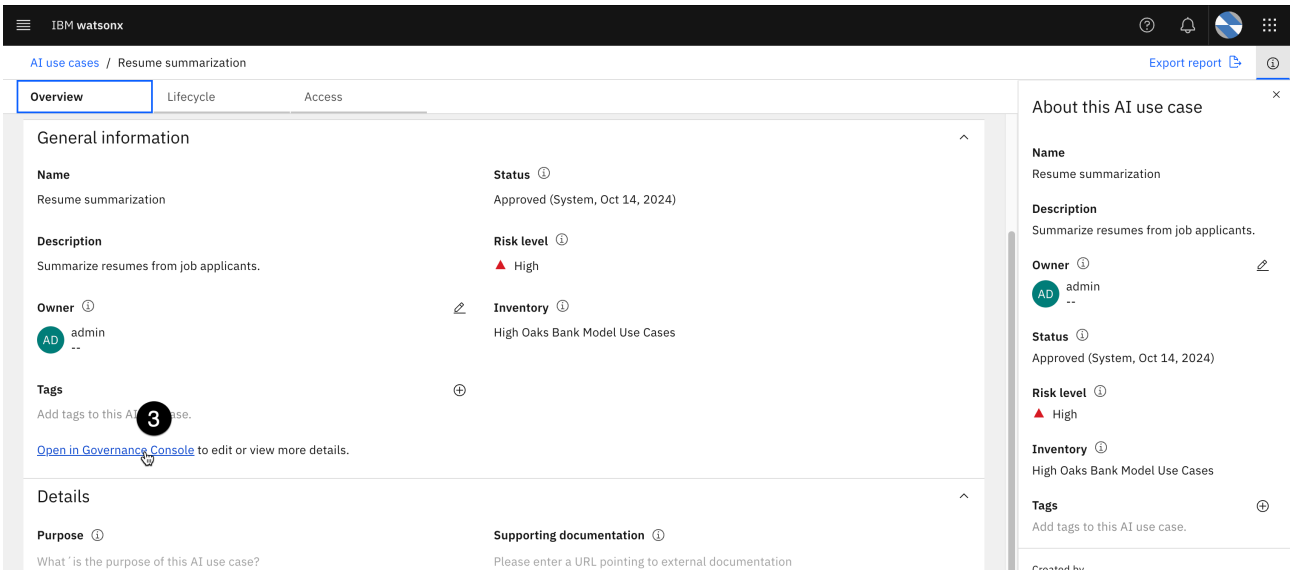
1. Scroll to the bottom of the factsheet and click on the More details button. A more detailed version of the AI factsheet opens, showing the model's position in the lifecycle, links to the development project, deployment spaces, and more.



2. From the Governance section, click on the View details button. The AI use case screen opens.



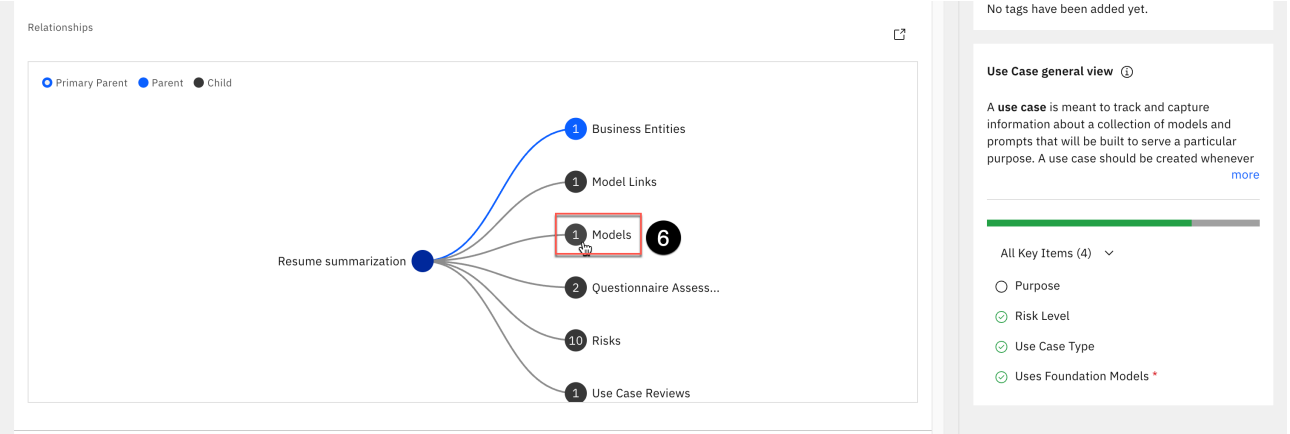
3. Scroll down to the General information section and click on the Open in Governance Console link. The watsonx governance console opens in a new tab and loads the model use case entry.



4. Scroll down to the Performance Monitoring section of the page. This section contains an overview of the metrics generated by the evaluation you ran in the previous step. The Metrics in Breach table shows all of the metrics whose values fell below the minimum acceptable thresholds.

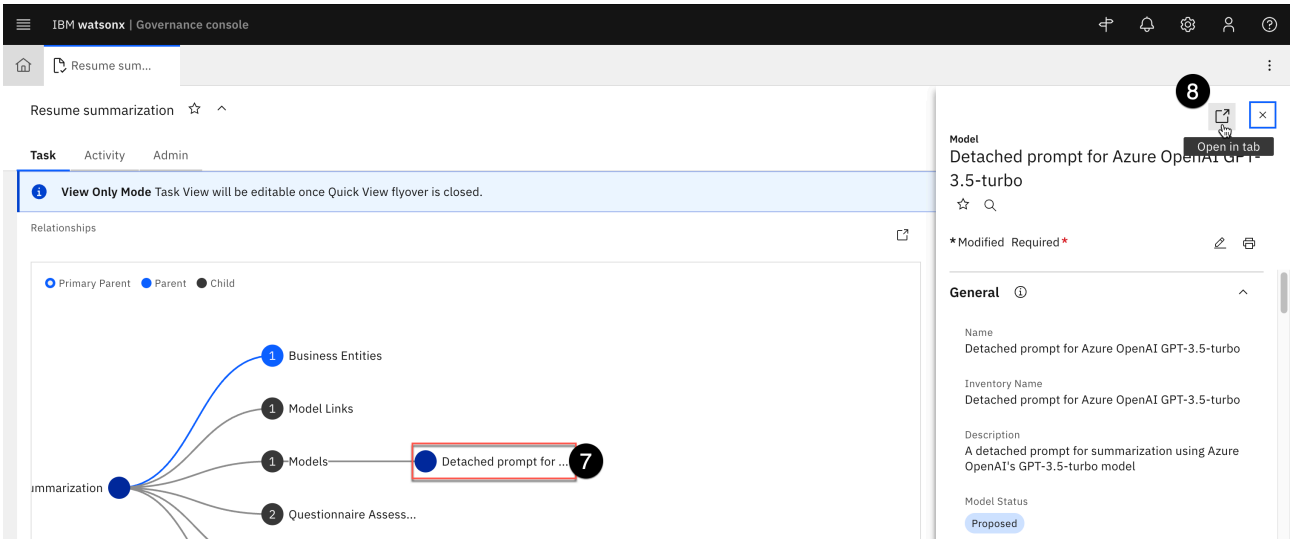
5. Scroll down to the Relationships section of the screen. Note that the Resume summarization parent node has one listed Model as child nodes.

6. Click on the circle for the Models node to expand it.



7. The resume summarization model you created and assigned to the use case is listed here. Click on it. The Model information panel opens on the right, showing the model details.

8. Click on the Open in tab button at the top right of the panel. The model will open in a new tab in the governance console.



9. Scroll down to the Associations section of the window and click on the Deployments tab. Note that the tab contains a link to the deployment of the model that you created in a previous step.

At this point in the lab, you have created a questionnaire and customized a governance workflow. Acting as a stakeholder, you have proposed a model for development, and gone through the governance process. You have then deployed and evaluated a third-party model. Throughout the entire process, you have seen how the model metrics and metadata are automatically tracked and surfaced in a variety of locations, allowing risk managers, AI engineers, and other business stakeholders to collaborate on implementing generative AI projects.

Next, you will use that same governance model for predictive AI projects.

Govern predictive models

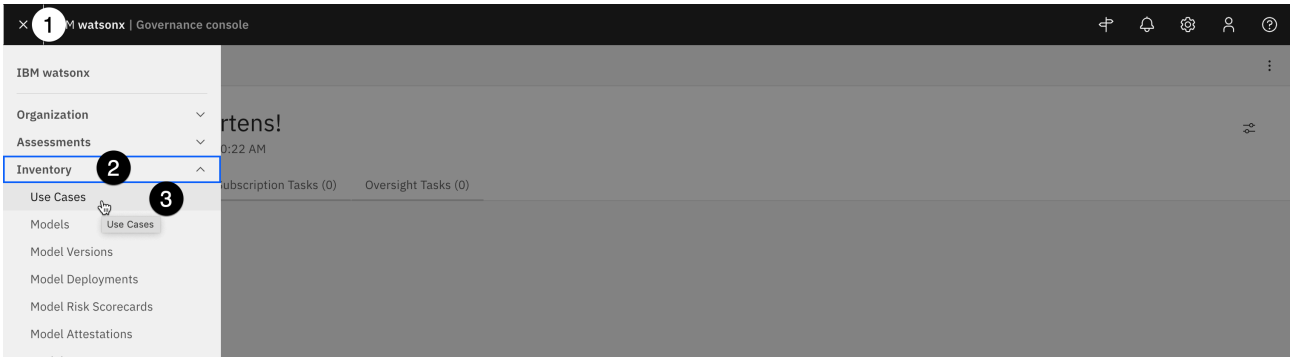
While much of the industry focus has been on ChatGPT and generative AI, the vast majority of models solving real-world business problems in production are traditional predictive machine learning models. Most organizations would significantly benefit from a governance solution for their predictive models, particularly given the increased regulatory environment.

In this section of the lab, you will evaluate a model that makes hiring recommendations for the HR department, which is running on Amazon SageMaker.

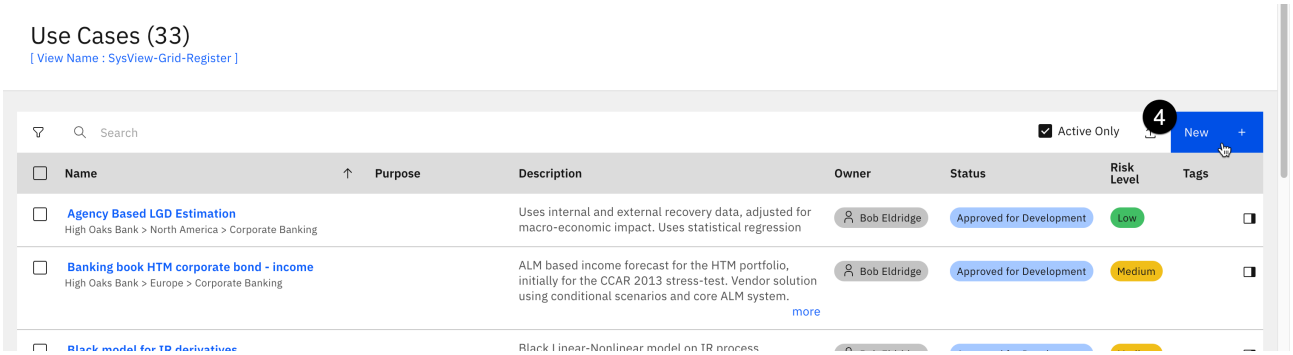
1. Create a predictive model use case

In the day 1 lab you created a sample use case and tracked the request through the approval process, including the risk and applicability assessment questionnaires. For this lab, you will once again create a use case request, but will skip several of the steps you completed previously.

1. Click on the hamburger menu in the upper left.
2. Click on the Inventory menu item to expand it.
3. Click on the Use Cases menu item. The Use Cases tab opens. Note that several sample uses cases were loaded by the lab administrator.



4. Click the blue New button. The New Use Case tab opens.



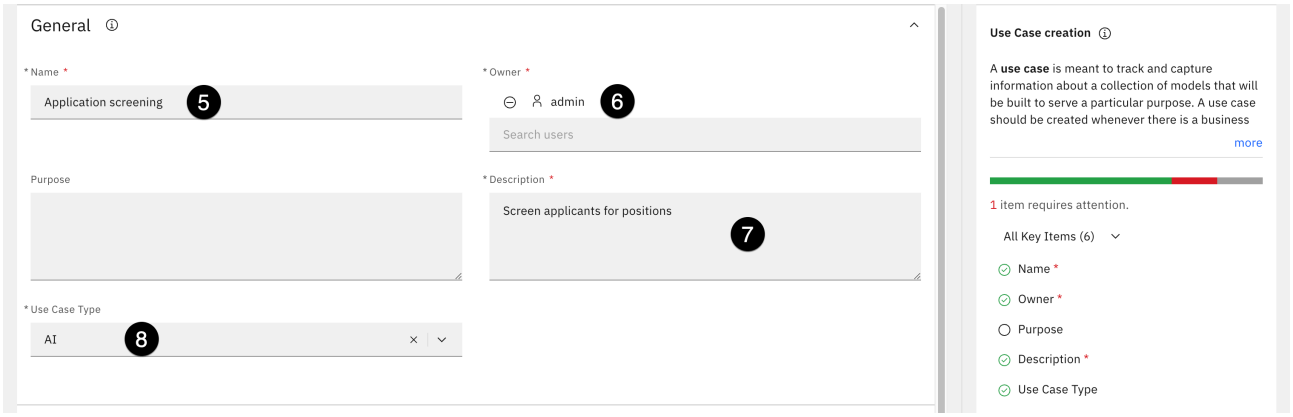
Note that the Model Use Case creation information panel on the right of the screen offers helpful information about model use cases, as well as a list of required fields. Clicking on any of the fields in that panel will scroll the screen directly to that portion of the form, helping you quickly rectify any items needing attention.

5. In the General section of the form, enter Application screening in the Name field. Note that when you enter a value in the field, the progress bar in the Model Use Case creation information panel updates.
6. Click the Owner field and enter the admin user into this field. DO NOT select any of the sample users that were loaded during the system configuration import step, as they will not have associated Cloud

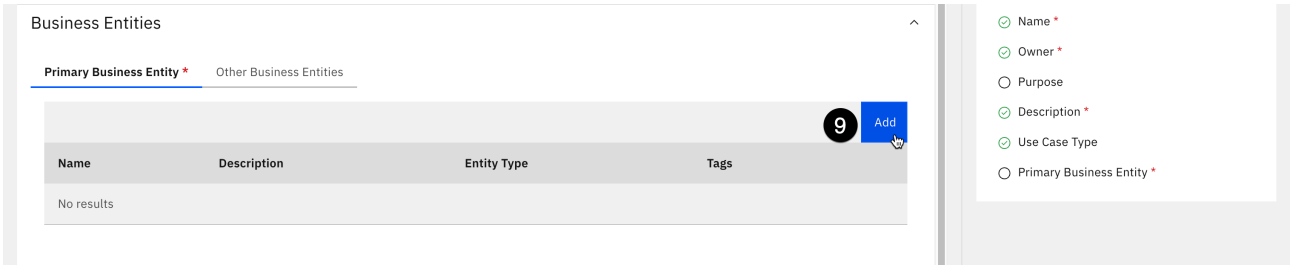
Pak for Data accounts and will not be able to log in and work with the use case.

7. Enter a description in the Description field.

8. Click on the Use Case Type dropdown and select AI.

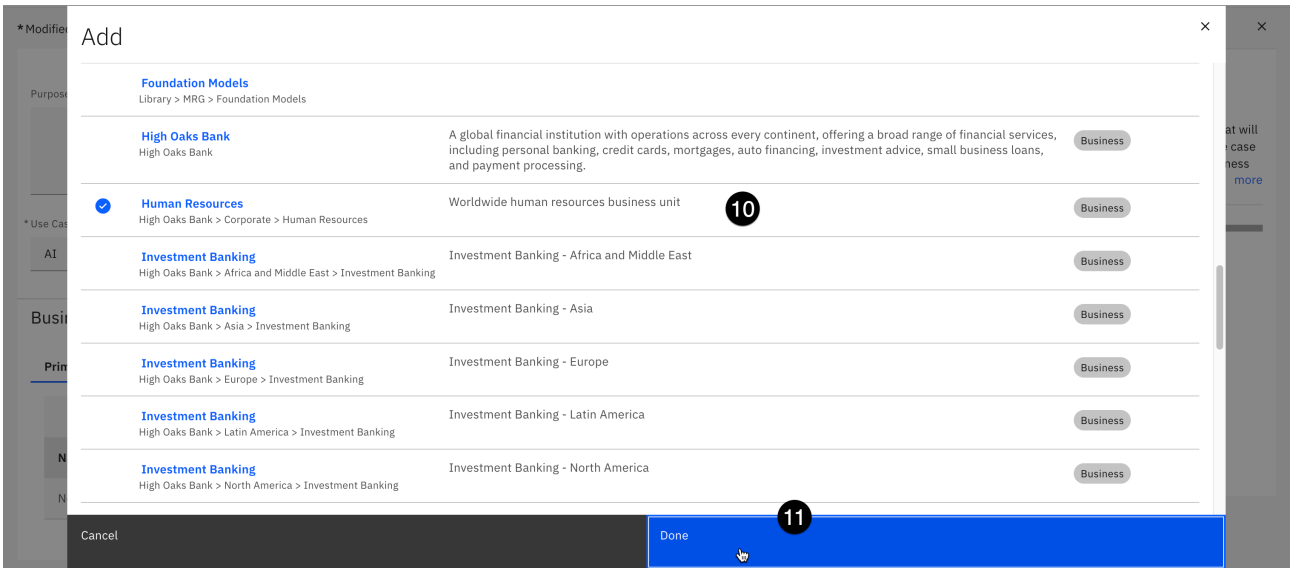


9. All model use cases are owned by business entities, representing the part of the organization responsible for requesting the use case. In the Business Entities section of the form, click the Add button. The Add window opens with a list of business entities defined for the organization.



10. Locate the Human Resources entity from the list and click on it to select it.

11. Click Done to add the business entity to the use case. The Add window closes.



12. Click the Save button in the upper right to save the use case.

When the use case has finished saving, the screen will reload with the view you customized in previous steps; you should see the Secondary EU AI Review field in the Regulatory Information section of the use case. At this point, the use case has been created and is now governed by the Use Case Request workflow that you modified. Specifically, it is in the Use Case Data Gathering stage of the workflow.

To progress the use case through the workflow, you will now need to perform the actions specified in the Action items in the workflow.

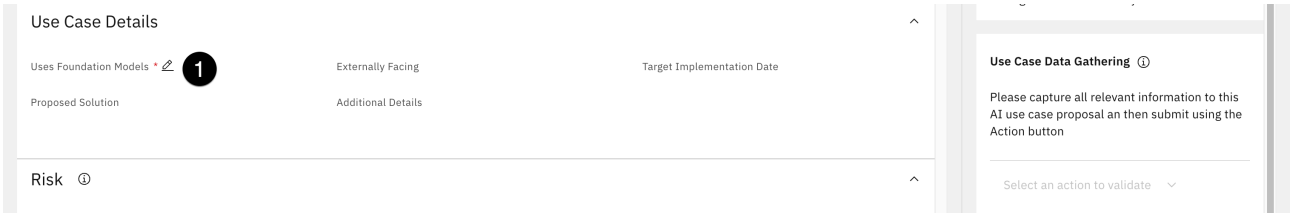
2. Progress the predictive model use case to the next phase

The use case request has progressed to the data gathering stage of the workflow, and has been assigned as an action for the appropriate owner. Recall that owners of each stage of the workflow can be configured, and alerts assigned.

In the day 1 lab you progressed a use case through the approval process, filling out the risk assessment questionnaire to identify possible risks. For the sake of time, in this lab you will use your administrator's authority to manually attach risks to the use case and then advance it to the proper lifecycle phase.

In an earlier section of the lab, you updated the model use case review to hold a new field (Secondary EU AI Review). When performing a PoX for your client, you may wish to add other fields to this view, which may contain other required information to be filled out in this stage. Information could include things like billing codes, additional documentation or justification, or more. In this case, you will only edit required fields specified in the information panel on the right before progressing to the next stage of the workflow.

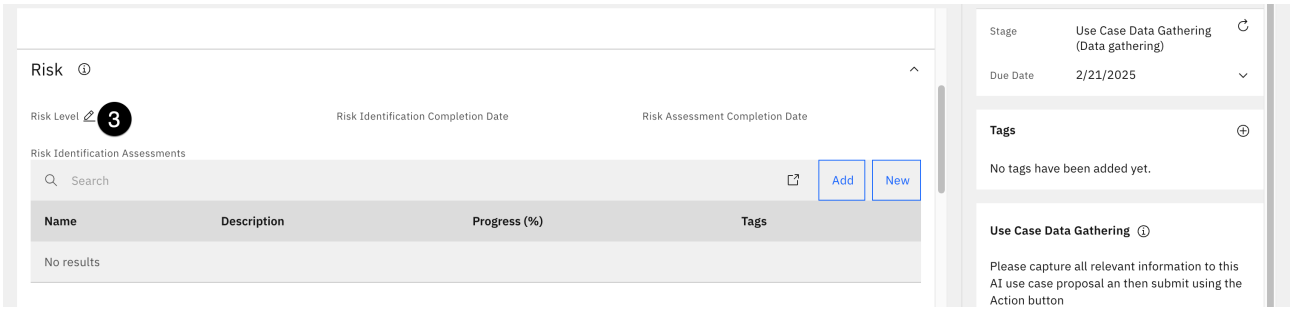
1. Scroll to the Use Case Details section of the view and click on the pencil icon that appears when you hover your mouse over the Uses Foundation Models field.



2. Use the dropdown to set the field to No.

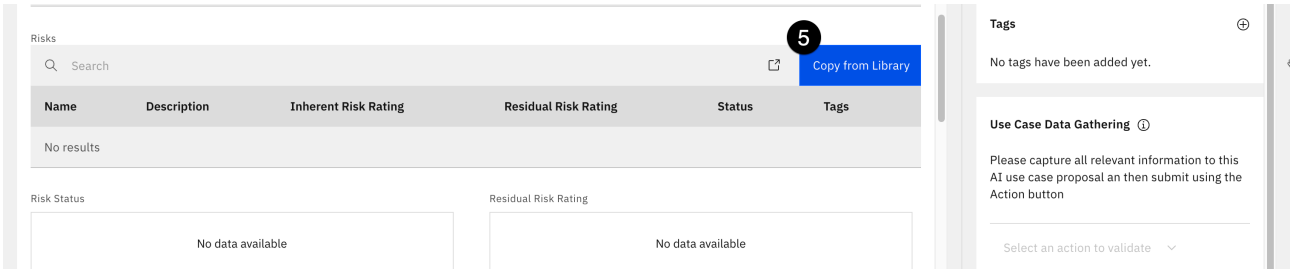
Risk Level represents the risk to the organization should issues arise with the models used to address the requirements laid out by the use case. A full risk assessment is beyond the scope of this lab; however, because hiring and employment violations can lead to expensive litigation damage to an organization's reputation, this use case will be marked as high risk.

3. In the Risk section of the form, click on the pencil icon next to the Risk Level field to edit it.



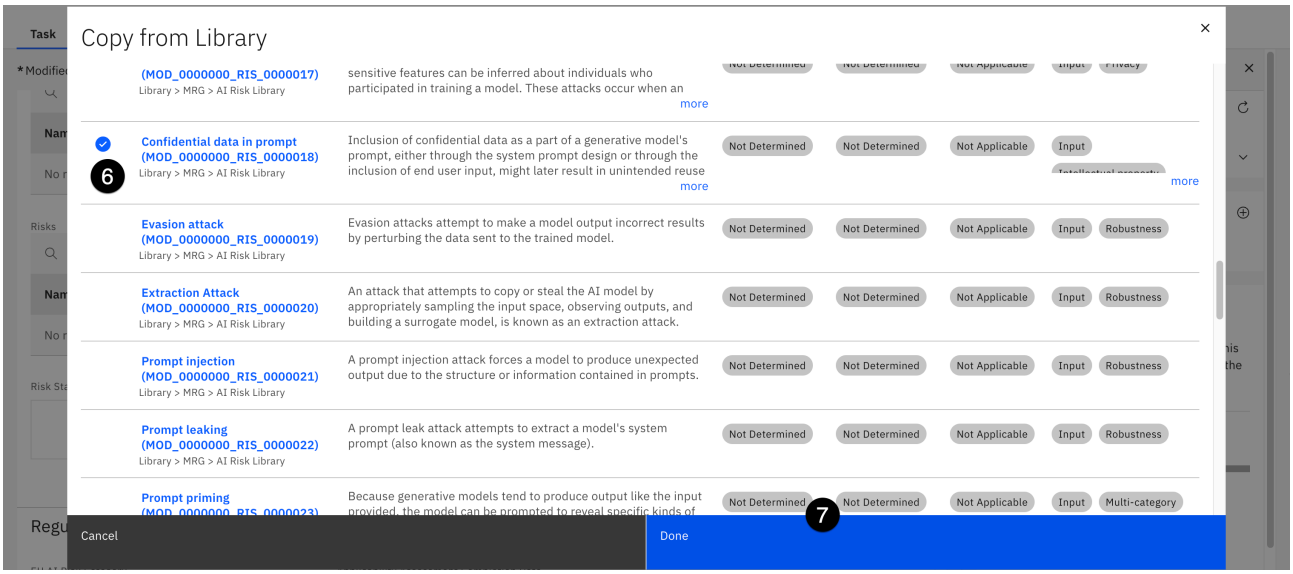
4. Select High from the dropdown.

5. Scroll down to the Risks table in the same section and click on the Copy from Library button. The Copy from Library dialog window opens, listing all the available risks currently in the library.



6. Scroll down to the Confidential data in prompt risk and click on it to select it.

7. Click on the Done button to add this risk to your use case.

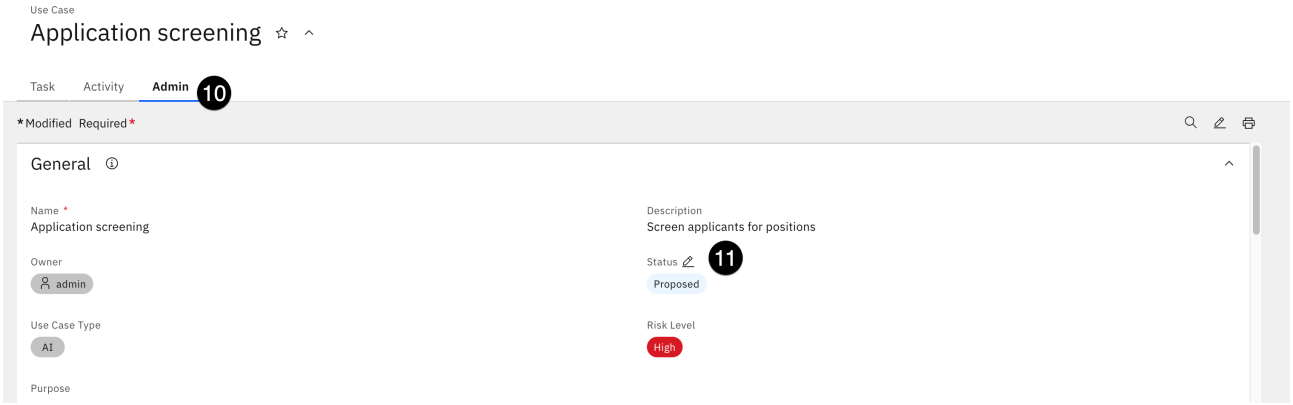


8. Repeat steps 5-7 for any other risks you wish to attach to your use case.

9. Click on the Save button in the upper right to save your use case. Note that if you see an error message saying that the use case has recently been updated by another user, you may need to refresh the page and verify that they information added to the form in previous steps has been saved, then click on the Save button again.

10. From the top of the view, click on the Admin tab.

11. Click on the pencil icon that appears when you hover your mouse over the Status field in the General section.



12. Use the dropdown to set the Status field to Approved for Development.

13. Click on the Save button to save your changes.

14. Click on the Task tab to return to the Task view of the use case.

At this point in the lifecycle, the model use case has been created, reviewed for risks, and approved by the various stakeholders. Personas involved are mostly non-technical, from the business user who requested the model to the risk and compliance officer who evaluated it. Next, the model would be developed by teams of data scientists and AI engineers. In this case, the model has been developed by a team using the Amazon SageMaker development platform, and deployed there as a candidate model for the use case.

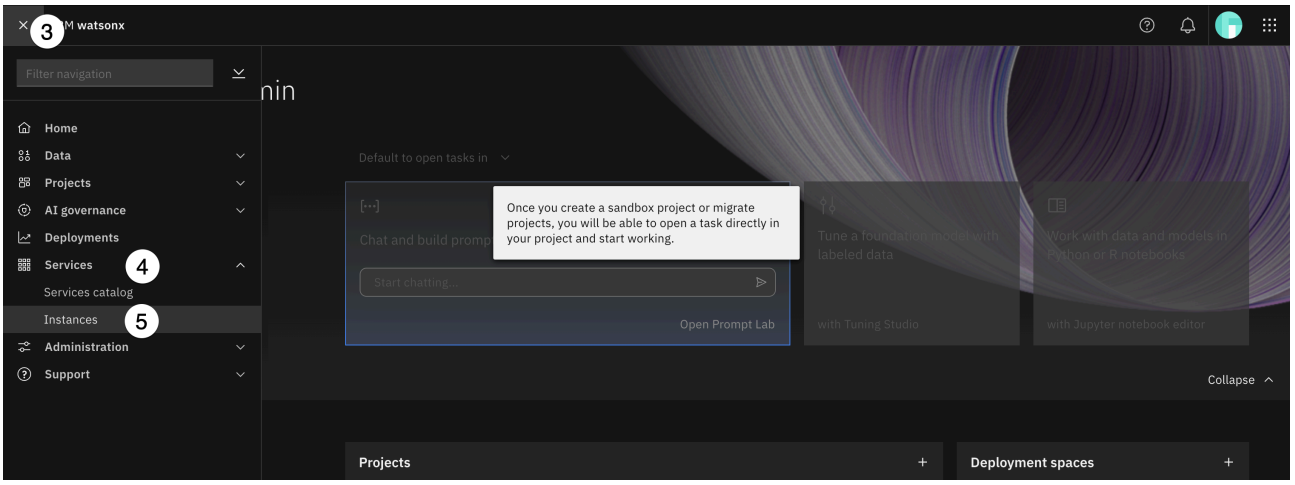
In the next steps of the lab, you will connect watsonx.governance to this model and configure it for evaluations.

3. Open the watsonx monitoring dashboard

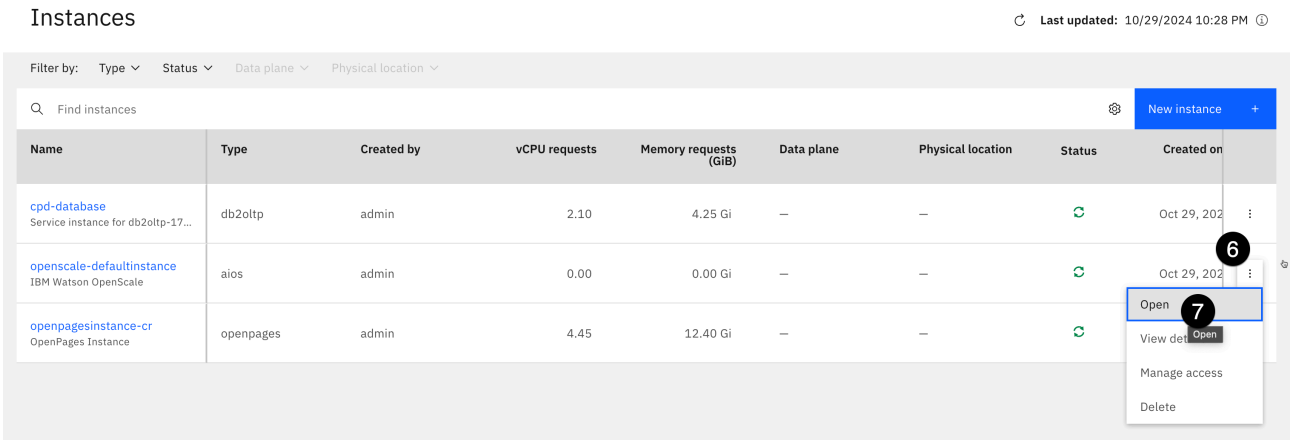
You can add Amazon SageMaker as a model provider from the watsonx monitoring (OpenScale) dashboard.

1. From the governance console, click on the hamburger menu in the upper left.
2. Click on the IBM watsonx menu item. The watsonx home screen opens.

3. Click on the hamburger menu in the upper left.
4. Click on the Services menu item to expand it.
5. Click on the Instances menu item. The Instances screen opens.

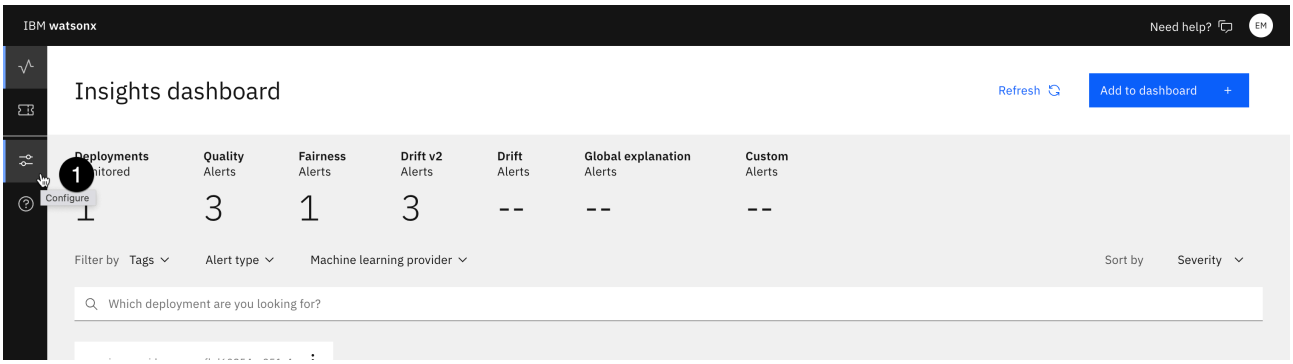


6. Locate the openscale-defaultinstance item in the table, and click on the three vertical dots to the right of it to open the context menu.
7. Click on the Open menu item. The watsonx monitoring dashboard opens.



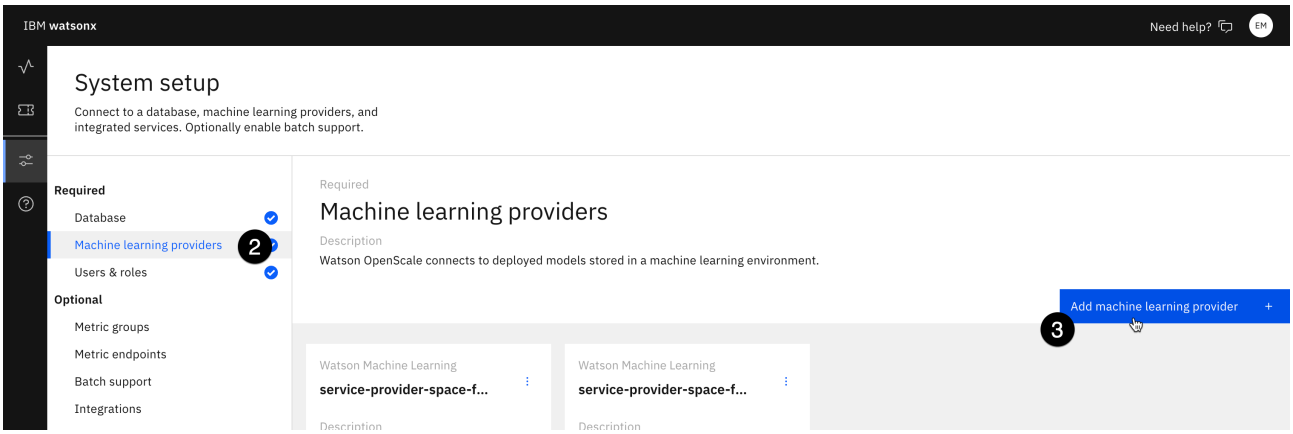
4. Add the SageMaker model to the dashboard

1. From the watsonx monitoring (OpenScale) Insights dashboard, click on the Configure button. The System setup screen opens.

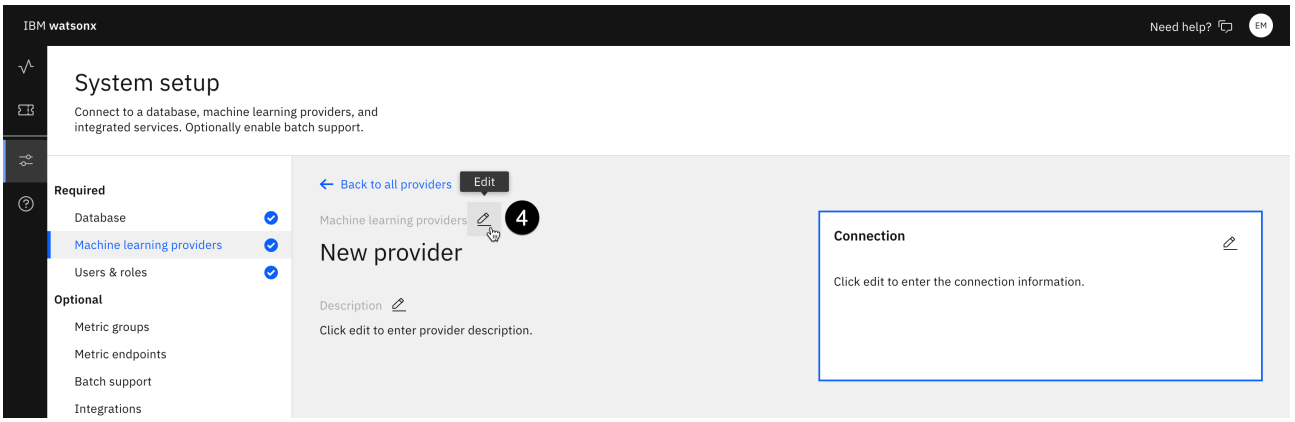


2. From the Required section in the left panel, click on Machine learning providers.

3. Click on the Add machine learning provider button.



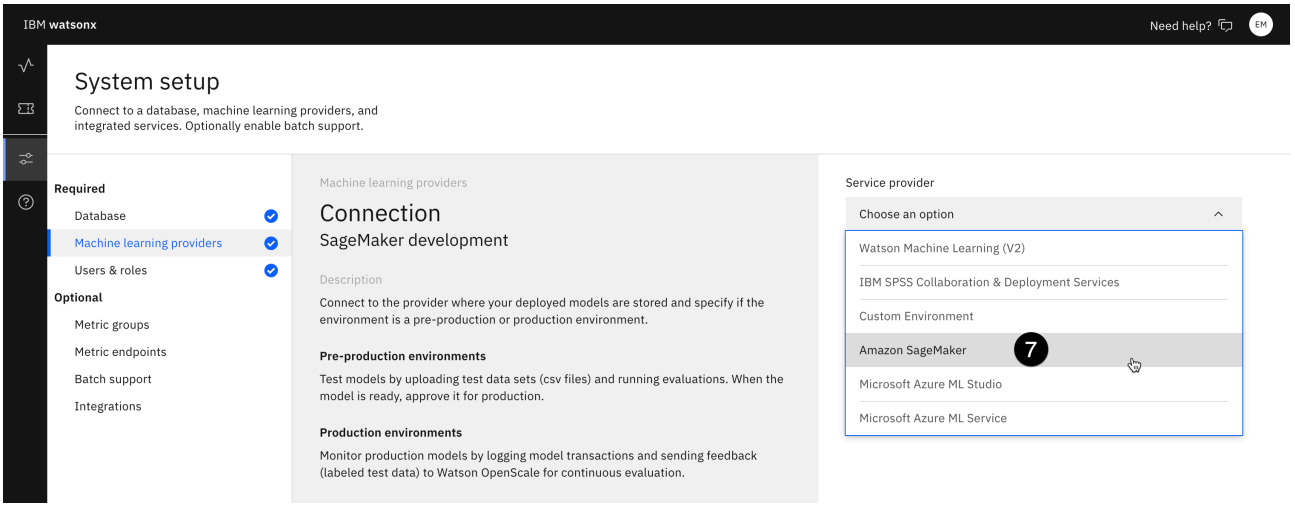
4. Click the Edit button for the Machine learning providers to edit the provider name.



5. Enter SageMaker development in the text field and click the Apply button.

6. Click on the Edit button in the Connection tile. The Connection panel opens.

7. Click on the Service provider dropdown. Note the different pre-built connectors available, including Microsoft Azure ML Studio and Microsoft Azure ML Service. Select Amazon SageMaker from the list.

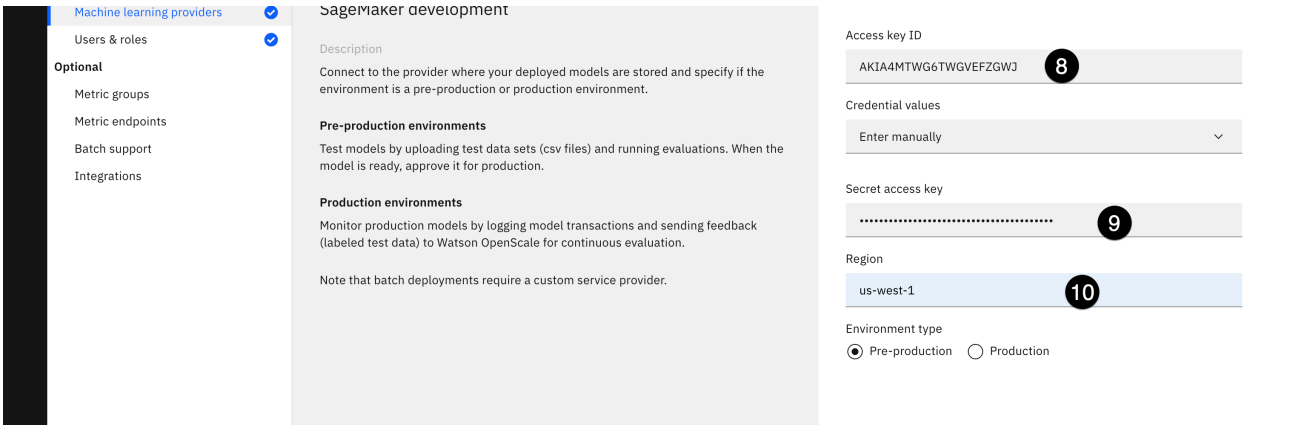


Enter your SageMaker credentials, which will be provided by your lab instructor.

8. In the Access key ID field, enter the AWS_ACCESS_KEY_ID value.

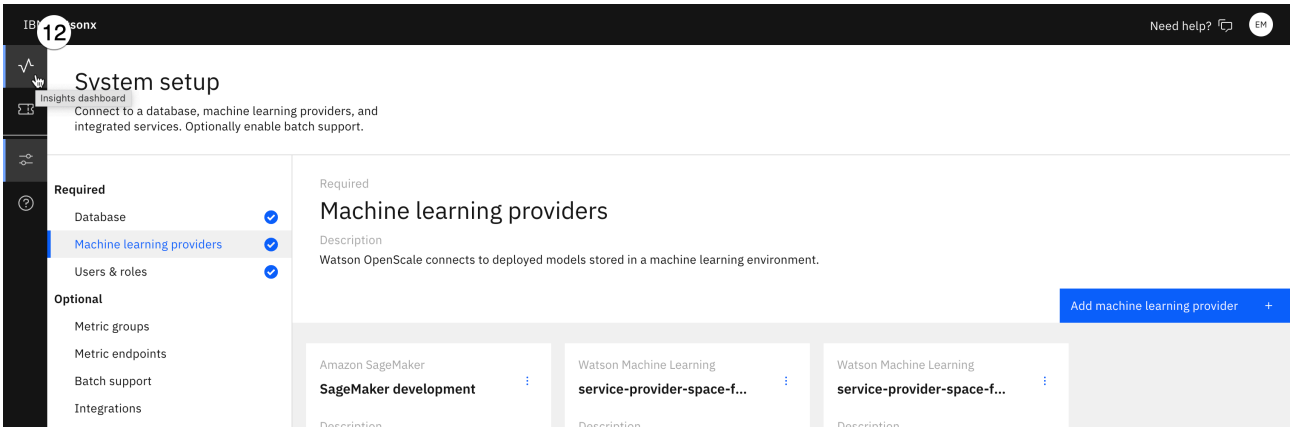
9. In the Secret access key field, enter the AWS_SECRET_ACCESS_KEY value.

10. In the Region field, enter the Region value.



11. Click on the Save button to save the SageMaker service as a machine learning provider for watsonx.governance.

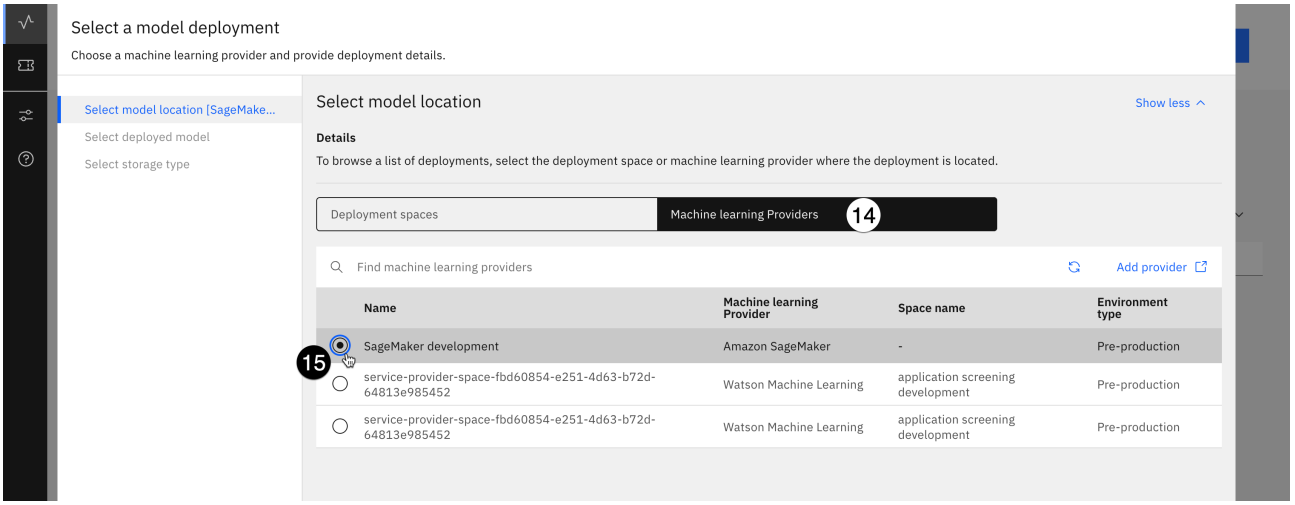
12. Click on the Insights dashboard button to return to the dashboard.



13. Click on the Add to dashboard button. The Select a model deployment window opens.

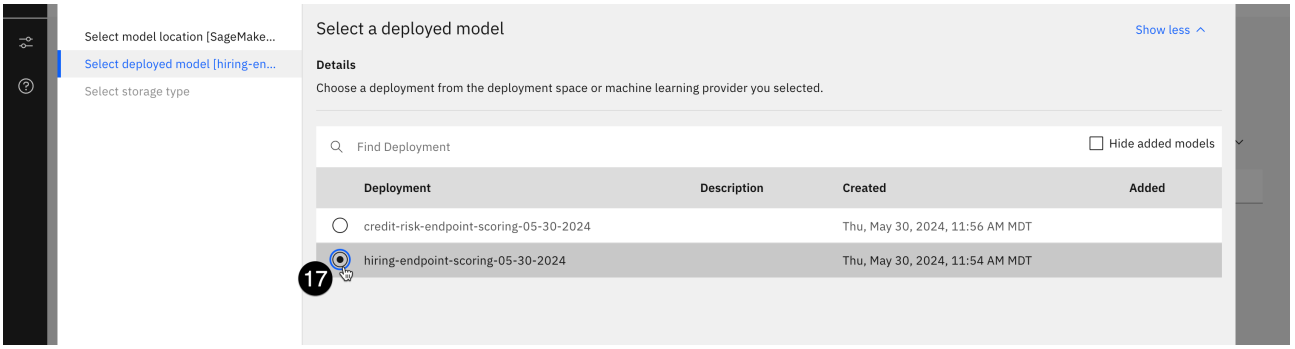
14. In the Select model location section, click on the Machine learning Providers button. A list of providers appears.

15. Click on the SageMaker development provider from the list.



16. Click on the Next button. The monitoring service will query the SageMaker service using the credentials you provided to get a list of deployed model endpoints.

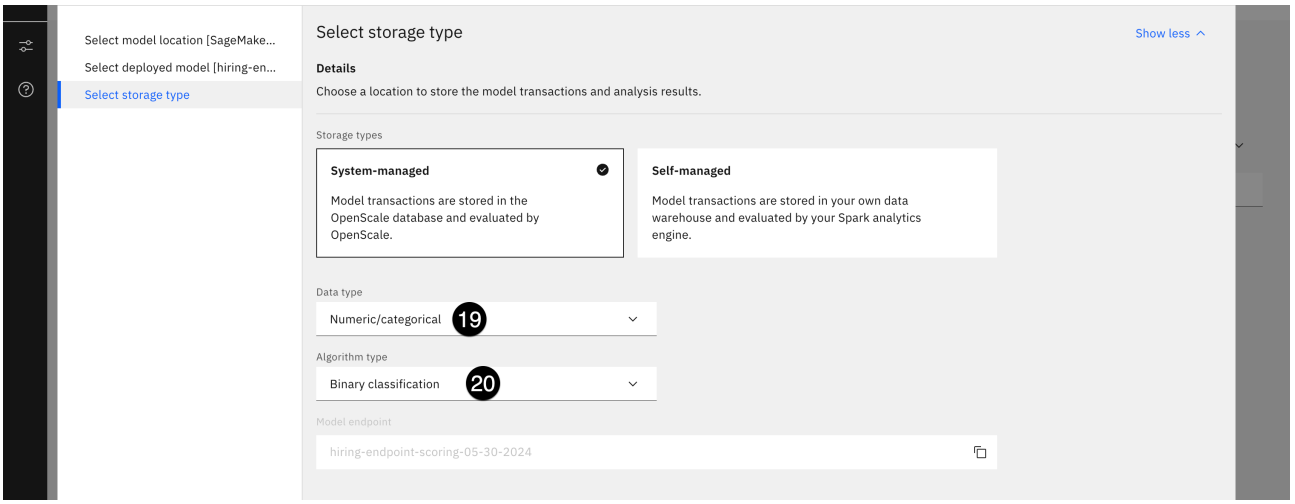
17. Click on the hiring-endpoint-scoring... deployment from the list.



18. Click on the Next button. The Select storage type window opens.

19. Click on the Data type dropdown and select Numeric/categorical from the list.

20. Click on the Algorithm type dropdown and select Binary classification from the list.



21. Click on the View summary button.

22. Click on the Save and continue button to add the deployed model to the dashboard. The Configure hiring-endpoint... screen opens.

5. Configure the SageMaker monitors

Next, you will configure the SageMaker model information and monitors.

1. Leave the Configuration method set to Manual setup and click on the Next button. The Specify training data window opens.

2. Right-click the link to download the hiring_training_data.csv file to your machine, then drag and drop it into the upload section on the screen, or browse to it.

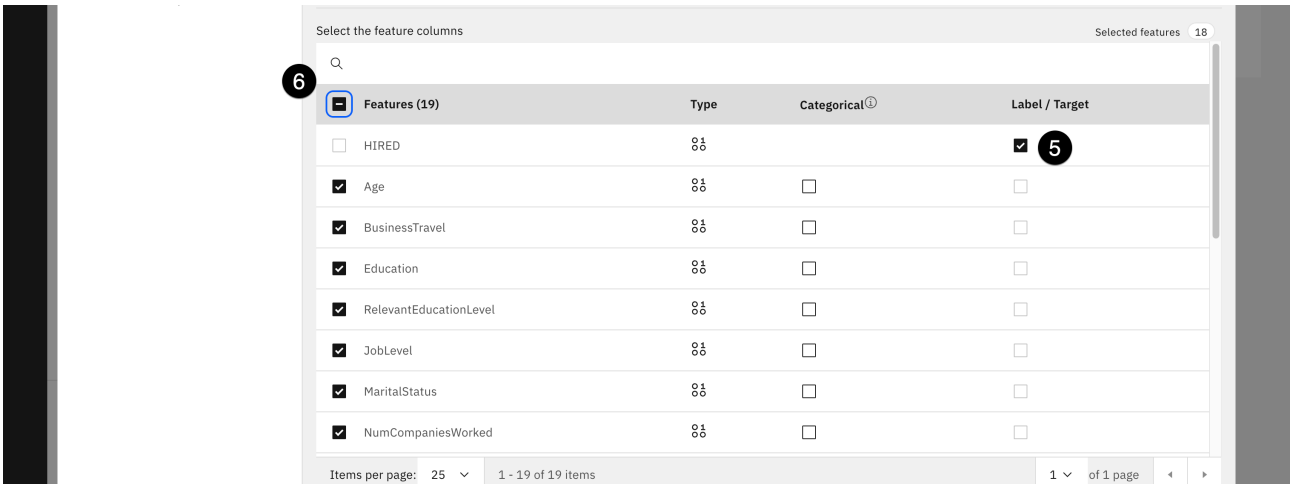
> Note: When downloading the file, your browser may change the file extension from *csv* to *txt*. If it does so, you will need to change the extension back to *csv*.

3. Click on the Select delimiter dropdown and select the Comma (,) option from the list.

4. Click the Next button. The monitoring service reads the CSV file. The Select the feature columns and label column screen opens.

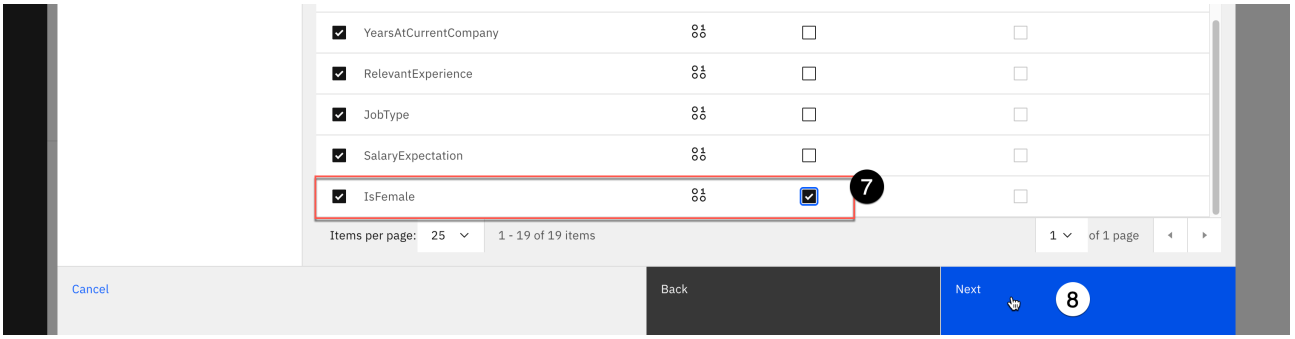
5. Check the Label / Target box for the HIRED column.

6. Check the box in the table header row to select the remaining columns as features.



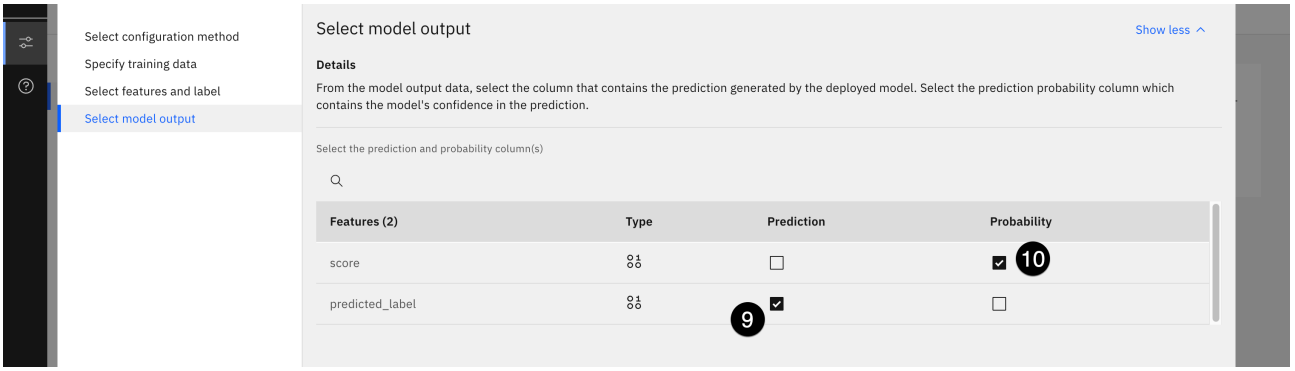
7. Scroll to the bottom of the table and check the Categorical box for the IsFemale feature.

8. Click on the Next button. The monitoring service queries the model to determine the structure of its output. The Select model output screen opens.



9. Check the Prediction box for the predicted_label field.

10. Check the Probability box for the score field.



11. Click on the View summary button.

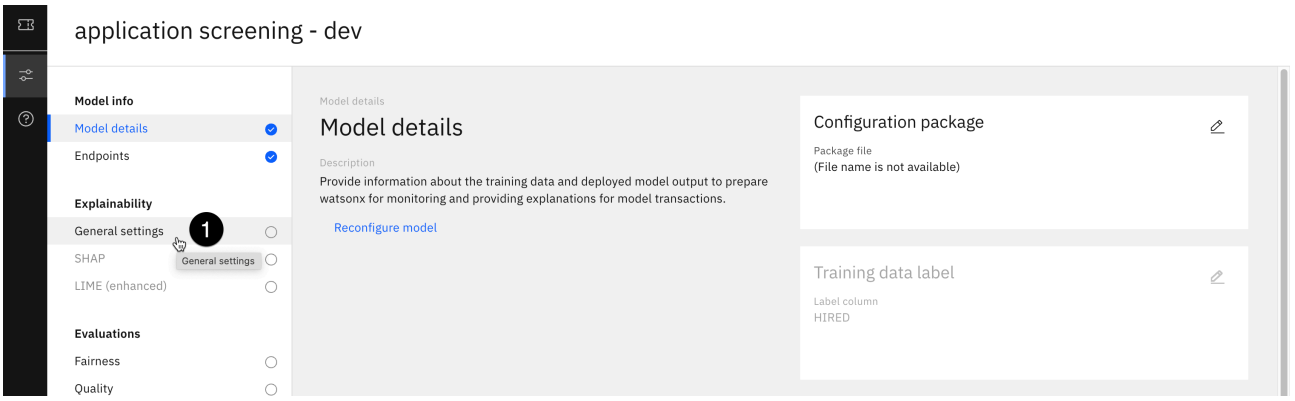
12. Click on the Finish button to finalize your configuration.

In the next steps, you will configure individual model monitors.

6. Configure explainability and fairness

Next, you will configure the explainability service and the fairness monitor.

1. In the Explainability section, click General settings.



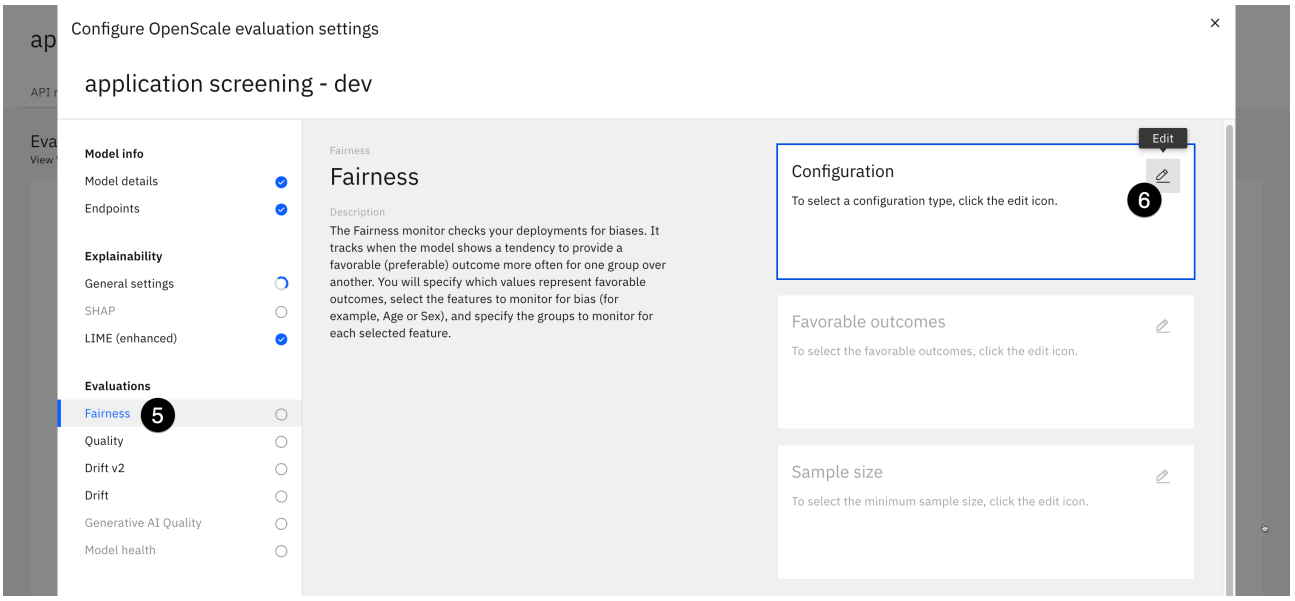
2. Click the Edit button in the Explanation method tile. Watsonx.governance offers two different algorithms to explain predictions: LIME (Local Interpretable Model-Agnostic explanations), and SHAP (SHapley Additive exPlanations).

3. Click the Next button to use the LIME method. The Controllable features panel opens.

4. You can designate certain features of the model as controllable, and can subsequently choose to include or exclude features that you cannot control when running an analysis. Use the switches to adjust controllable features as you wish, then click the Save button to save your choices.

5. From the Evaluations section in the left panel, click on Fairness.

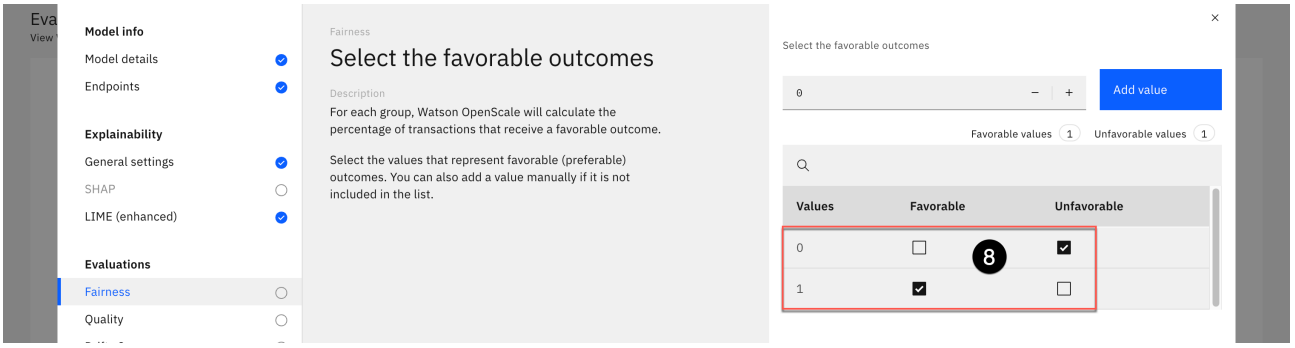
6. Click on the Edit button in the Configuration tile.



7. The Configure manually configuration type has been selected. Click on the Next button.

To monitor fairness, you need to identify favorable and unfavorable outcomes, as well as monitored and reference groups. In this particular model, 1 represents a hiring recommendation, and is a favorable outcome. 0 represents a no-hire recommendation, and is unfavorable.

8. Use the checkboxes to mark 0 as Unfavorable and 1 as Favorable.



9. Click on the Next button. The Sample size screen opens.

10. Enter 100 in the Minimum sample size field. This will allow you to calculate evaluations without needing more than 100 rows of data.

11. Click on the Next button. The Metrics screen opens.

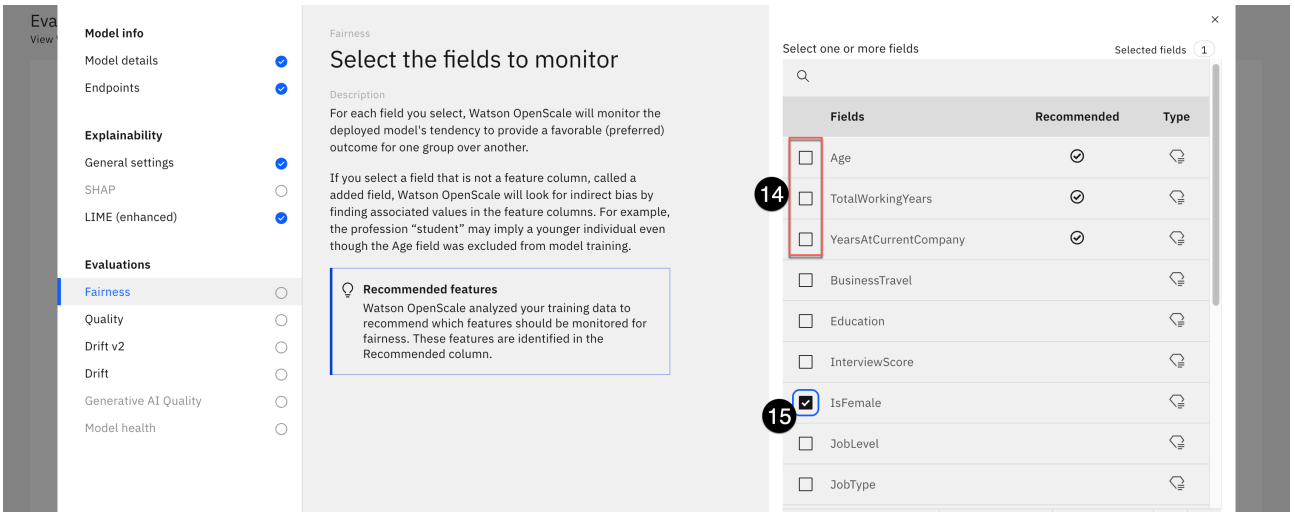
Multiple metrics are available for measuring fairness. Two of them (Disparate impact and Statistical parity difference) can be calculated at runtime strictly from data being submitted to the model. The others require feedback (ground truth) data. More information on the metrics can be found in the watsonx.governance documentation.

12. Click on the Next button.

13. The standard threshold for disparate impact is 80%, though it can be adjusted to meet specific requirements. Click on the Next button. The Select the fields to monitor screen opens.

14. IBM watsonx has analyzed the data and recommended different fields to monitor, including Age, TotalWorkingYears, and YearsAtCurrentCompany. For the purposes of this lab, uncheck each of those fields.

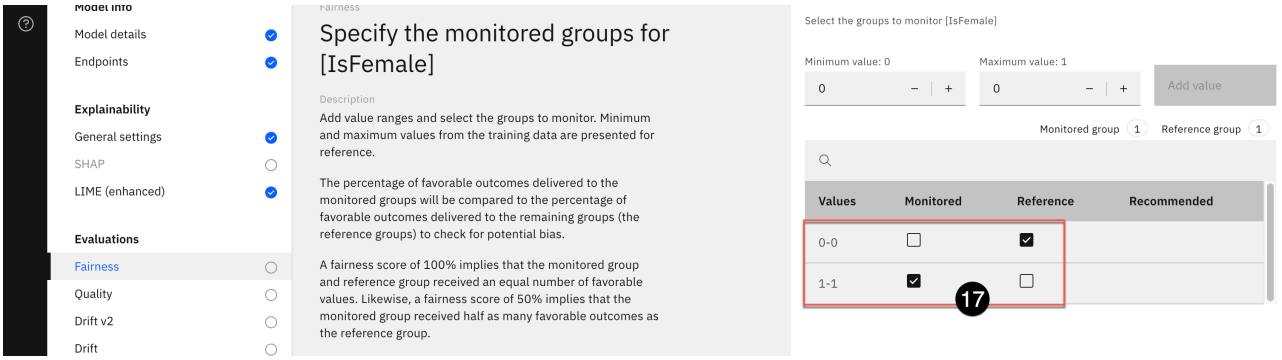
15. Scroll down in the table on the right and check the box to the left of the IsFemale item.



16. Click on the Next button.

In this model, females are denoted with a 1 in the IsFemale feature column, while males are denoted with a 0. Note that in a real-world example, you would use the indirect bias detection feature.

17. Click the checkboxes to designate the 0 value (0-0 range, males) as Reference group and the 1 value (1-1 range, females) as the Monitored group.



18. Click the on Next button.

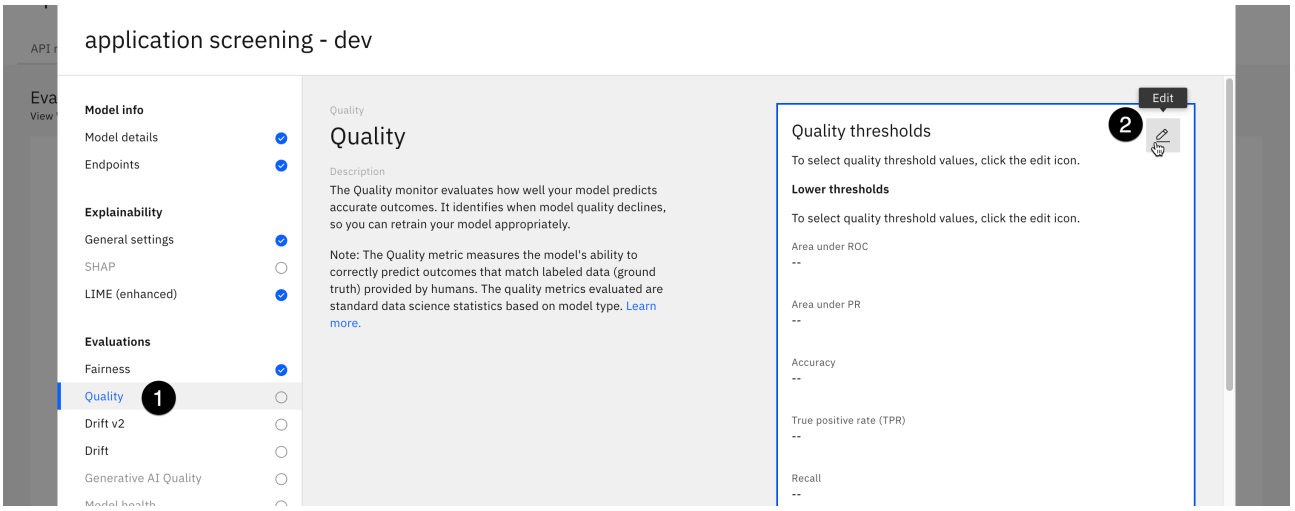
19. Note that you have the option to set different thresholds for each fairness monitor. Click on the Save button to save your fairness configuration.

7. Configure quality and drift

Next, you will configure the quality and drift monitors. Drift refers to the degradation of model performance due to changes in data or changes in relationships between input and output.

1. From the Evaluations section on the left, click on the Quality item.

2. Click on the Edit icon in the Quality thresholds tile.



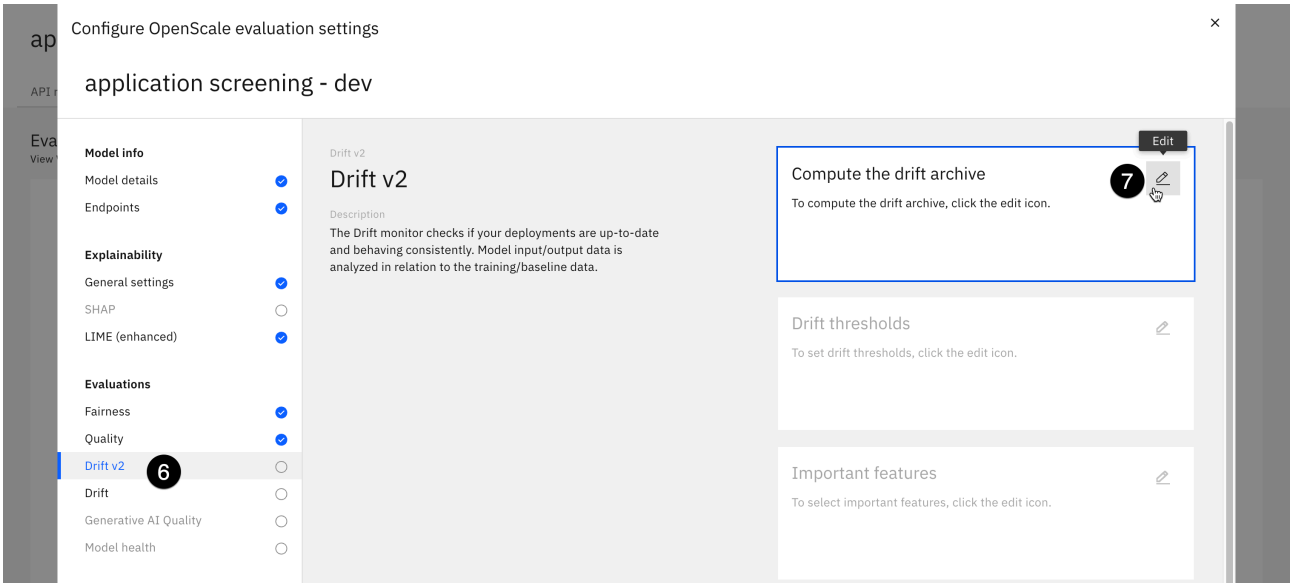
3. Over a dozen quality metrics are automatically calculated by watsonx.governance. You can find more information on each of them in the documentation. Click on the Next button to accept the default thresholds.

4. Enter 100 in the Minimum sample size field.

5. Click on the Save button to save your configuration.

6. From the Evaluations section on the left, click on the Drift v2 item.

7. Click on the Edit icon in the Compute the drift archive tile.

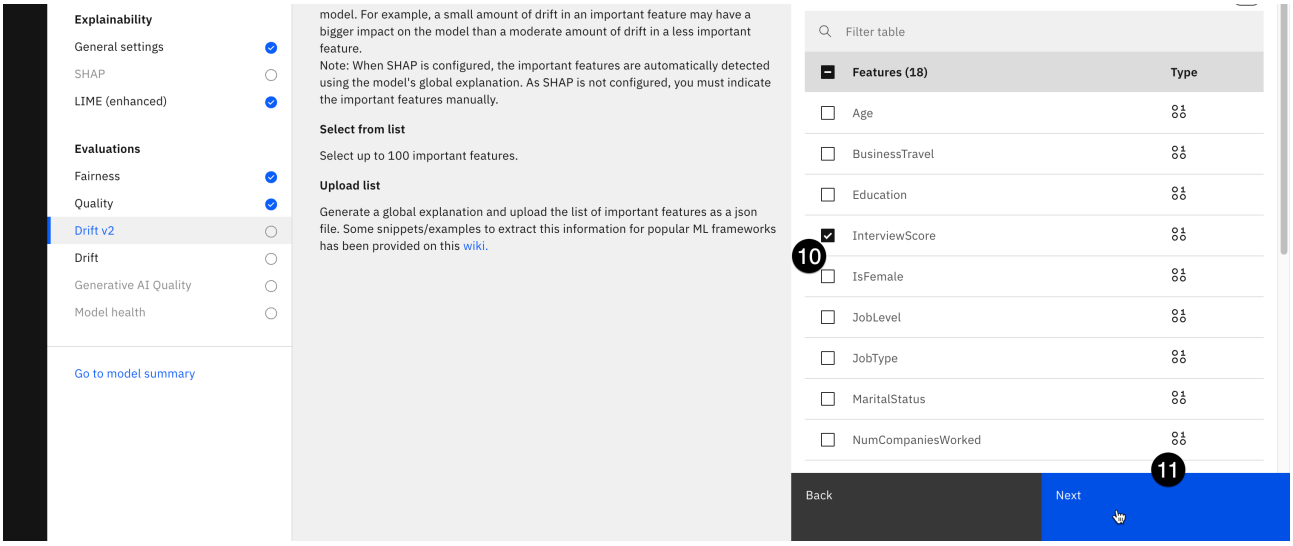


8. Because you uploaded the training data earlier when configuring the monitors, you now have the option to let Watson OpenScale compute the necessary statistics to measure drift. Click on the Next button.

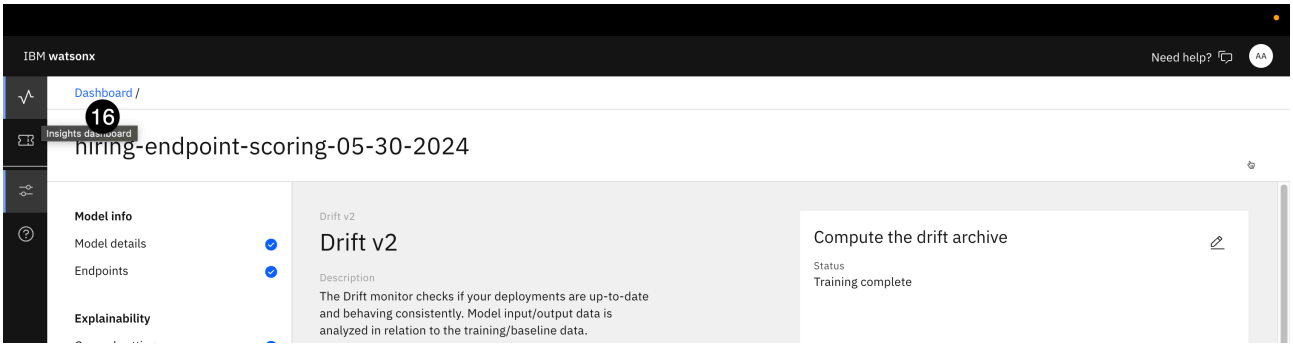
9. Leave the default drift thresholds set to their default values. Click on the Next button. The Important features screen opens.

10. When developing the model, data scientists will perform tests to see which features impact the model the most. For this model, those features are InterviewScore, YearsAtCurrentCompany, and SalaryExpectation. Locate those features in the list and check the boxes to the left of them to mark them as important.

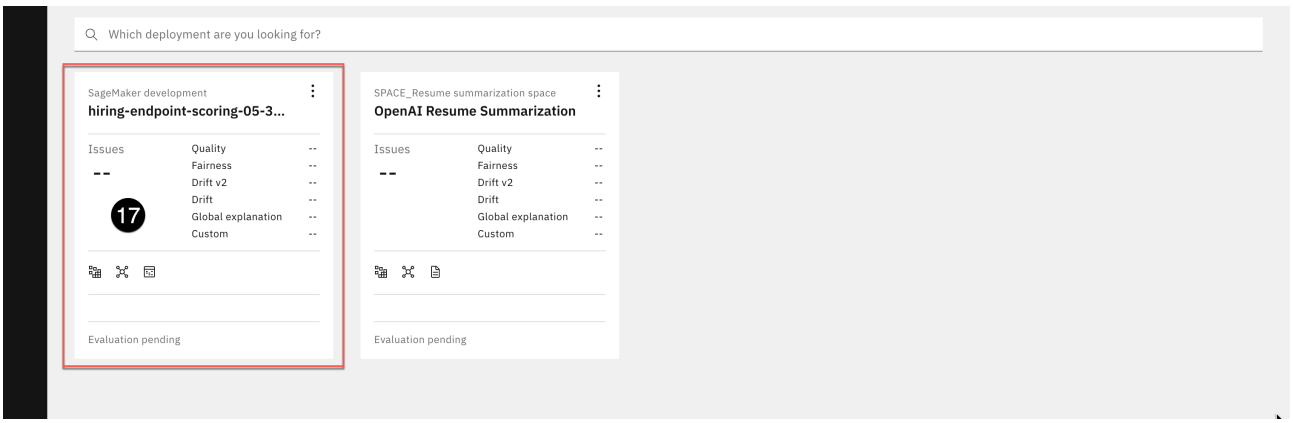
11. Once all the important features have been identified, click on the Next button to continue. The Most important features screen opens.



12. Check the box to the left of the most important feature (InterviewScore) to identify it.
13. Click on the Next button to continue.
14. Leave the Minimum sample size value set to its default and click the Save button. Watson OpenScale begins training the drift model in the background. This process can take up to five minutes. Once it has finished, the monitors will be fully configured and the model can be evaluated.
15. Click on the X button in the upper right to close the evaluation settings window.
16. Return to the Insights dashboard by clicking on the icon in the top left.



17. Locate the tile for the SageMaker model on the dashboard and click on it. The model information screen opens.

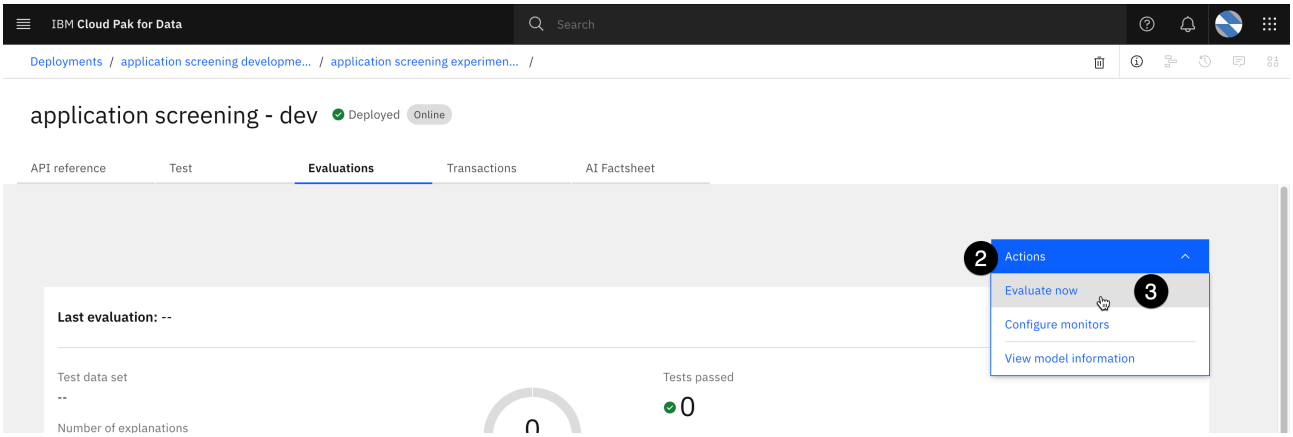


No current evaluations have been run on the model. In the next step, you will run one.

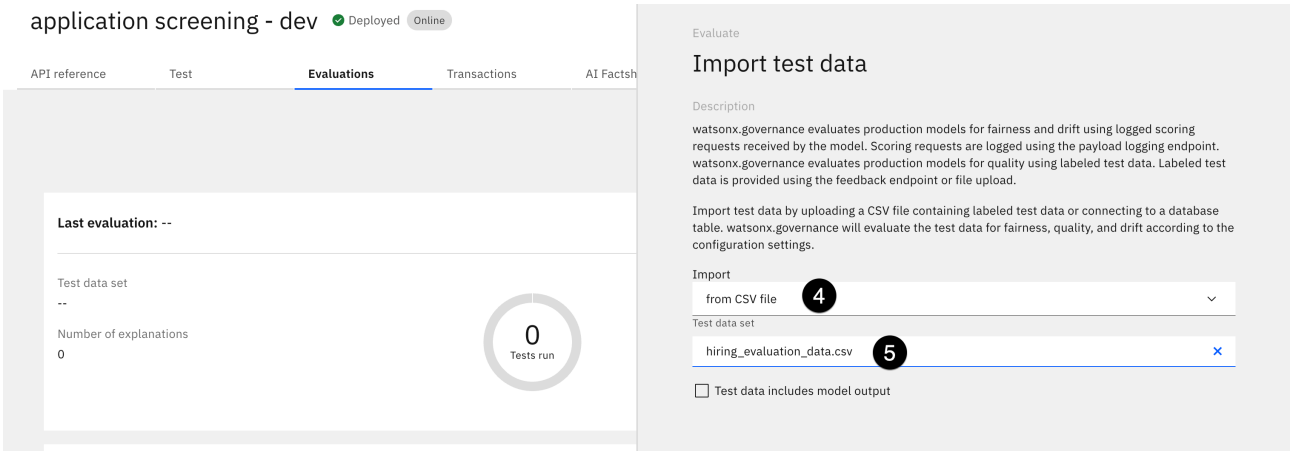
8. Evaluate the SageMaker model

Evaluation methods in watsonx.governance differ depending on whether the models are deployed to production spaces or pre-production spaces. Production models hosted in the same environment as watsonx.governance automatically register their input and output into the watsonx.governance datamart. Third-party production models can use a REST API to write their input and output into the datamart. Pre-production models are evaluated by uploading data in comma-separated value (CSV) files.

1. Right-click on the link for the hiring_evaluation_data.csv file and download it to your machine.
2. Click on the Actions button. The Actions menu opens.
3. Click on the Evaluate now menu item. The Import test data panel opens.



4. Click on the Import dropdown and select from CSV file.
5. Click the link to browse to the *hiring_evaluation_data.csv* file you downloaded in step 1.



6. Click on the Upload and evaluate button to begin the evaluation. Note that the evaluation can take up to five minutes to complete.
7. When the evaluation has finished, take a moment to review the results. The model has likely failed several tests. Clicking on the individual monitors provides further details.

9. Link the SageMaker model to the use case

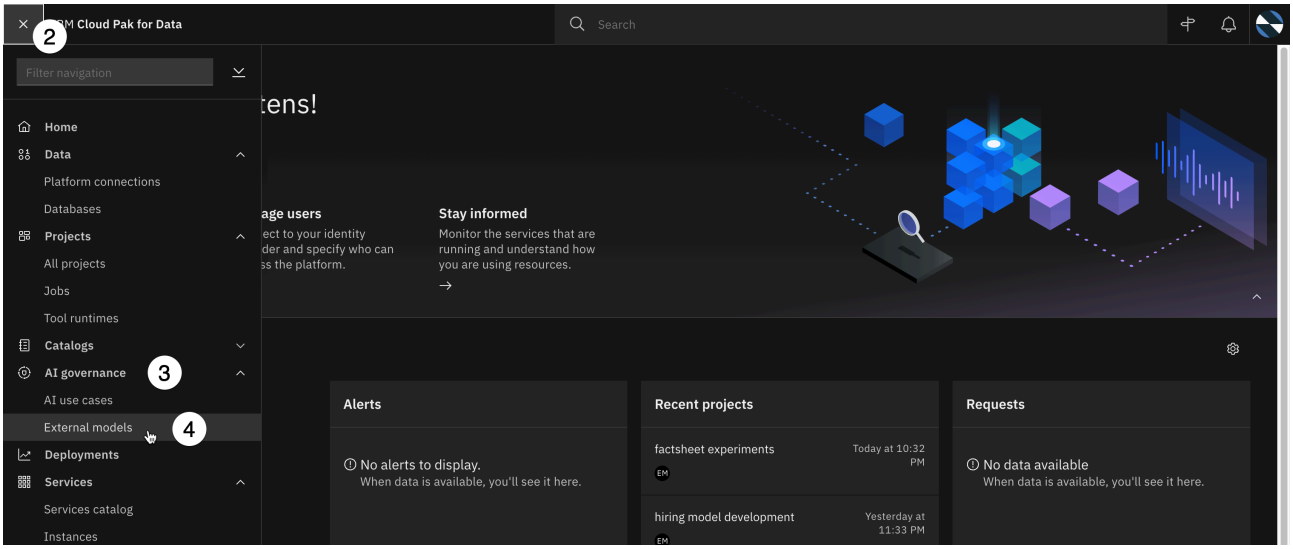
Now that the SageMaker model has been evaluated, it will appear in the External models page found in the AI governance menu.

1. In your browser, return to the watsonx / Cloud Pak for Data home screen. You can use the link provided by your lab instructor, or edit the URL in your browser's address bar to remove everything starting with *aiopenscale*.

2. Click on the hamburger menu in the upper left.

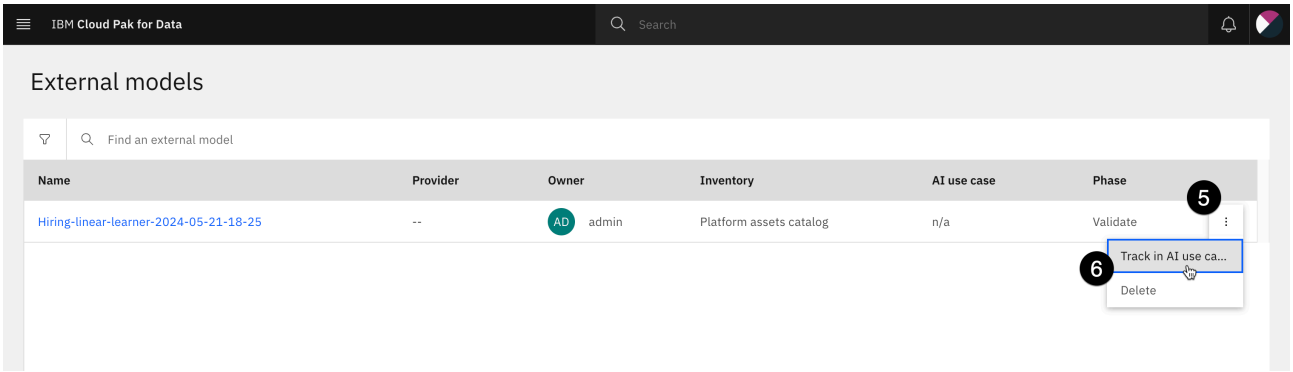
3. Click on the AI governance menu item to expand it.

4. Click on the External models menu item. The External models screen opens.

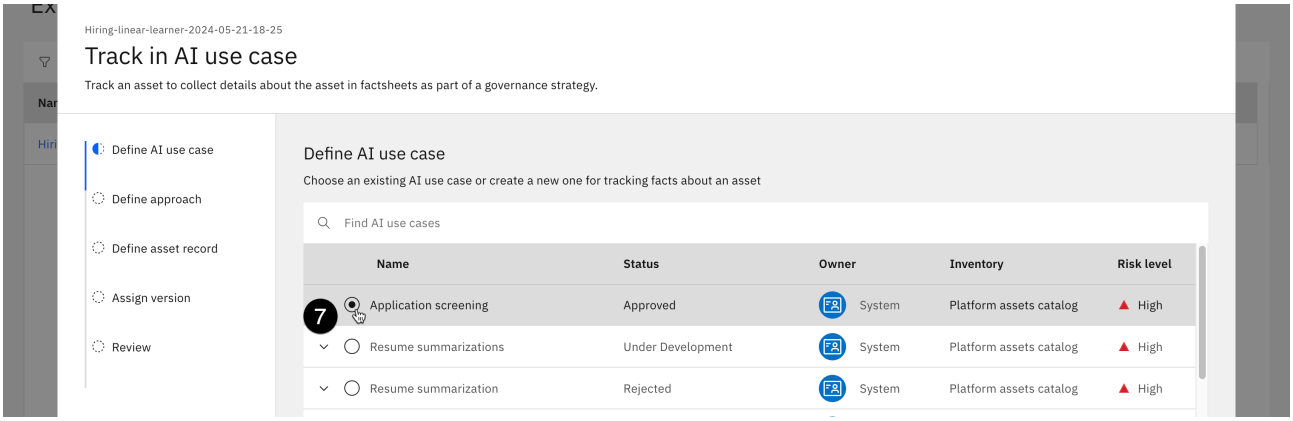


5. Locate the external hiring model in the list and click on the three vertical dots to the right of the model. The context menu opens.

6. Click on the Track in AI use case menu item from the context menu. The Track in AI use case window opens.



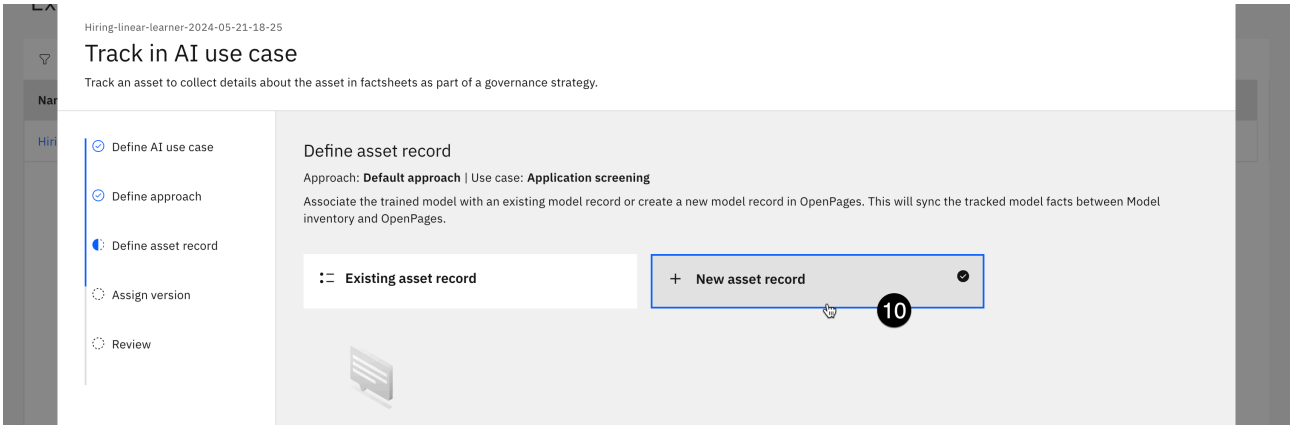
7. Locate the Application screening use case in the list and check the circle to the left of the use case name to select it.



8. Click on the Next button. The Define approach window opens.

9. Click on the Next button to accept the default approach. The Define asset record window opens.

10. Click on the New asset record tile to create a new record for the model in the inventory and the governance console.



11. Click on the Next button. The Assign version window opens. This screen allows you to set a version number for your model based on its progress in development.

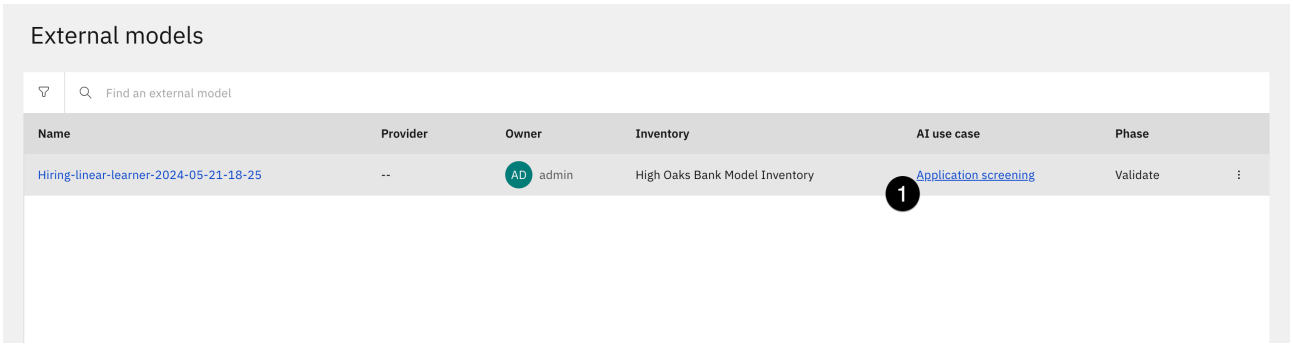
12. Click on the Next button. The Review window opens.

13. Click on the Track asset button to being tracking the asset in the use case. When the model has been successfully added to the use case, the external models table will update to reflect the new association.

10. View the model metrics in the use case

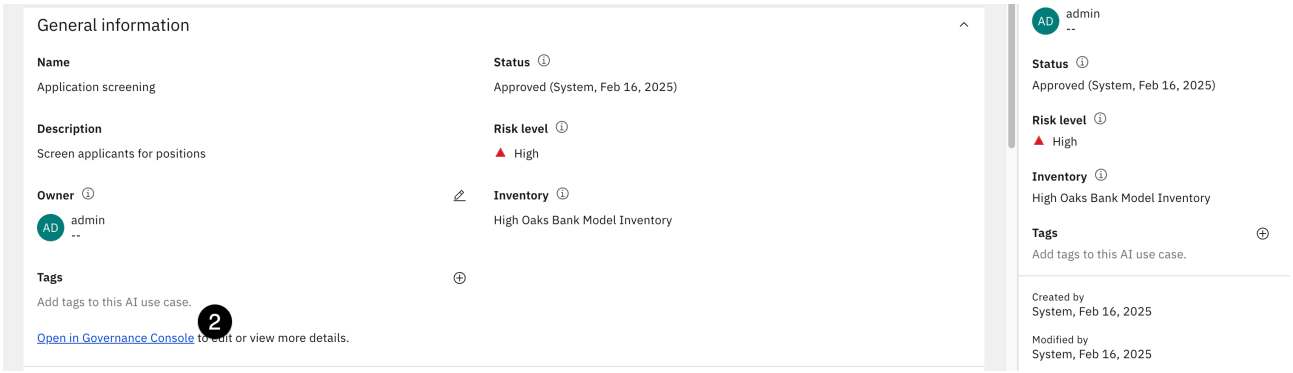
Next, you will view the use case and the gathered metrics in the governance console.

1. Click on the link for the Application screening use case. The use case will open.



This view of the use case is focused more on technical users, and looks different than the one in the governance console. However, all the information here is automatically synchronized with the governance console, to ensure that all stakeholders have the most up-to-date metrics and metadata.

2. Click on the Open in Governance Console link in the General information section of the use case view. The governance console opens and loads the view of the use case.



3. Scroll down to the Performance Monitoring section. Note that the metrics for both models are combined here, organized into breach status for major categories such as quality, fairness and more. You can explore the metrics in detail, clicking into each to find more information.

Note that you can also view the model metrics, and the updates made to the model lifecycle, in the model factsheet. The factsheet can be found in the AI use cases page of the AI governance section of Cloud Pak for Data.

Metrics data is generated by the watsonx.governance monitoring service (OpenScale), and automatically written to the factsheet, then automatically updated in the governance console. In this way, data is always kept in sync and stakeholders automatically receive the most current information in the format that is most useful for them.

Conclusion

Congratulations, you have completed the watsonx.governance hands-on lab. In this extensive lab, you saw how the governance console could be configured to meet the individual needs of an organization, and how it helps define, automate, and enforce best practices in approval workflows.

You saw how to create questionnaires, and how those questionnaires can be used to perform actions like associating risks with model use cases or prompting additional reviews.

You then created a pair of model use cases, and took them through the approval process.

Next, you oversaw the model lifecycle, including metrics gathering, for a generative models on Microsoft Azure. You then did the same for predictive models on Amazon SageMaker. You saw how the metrics evaluations of those models were automatically updated in multiple platforms, from factsheets to the governance console, to provide the right information to the right stakeholder at the right time without any additional effort from data science teams, or any reliance on manual processes.