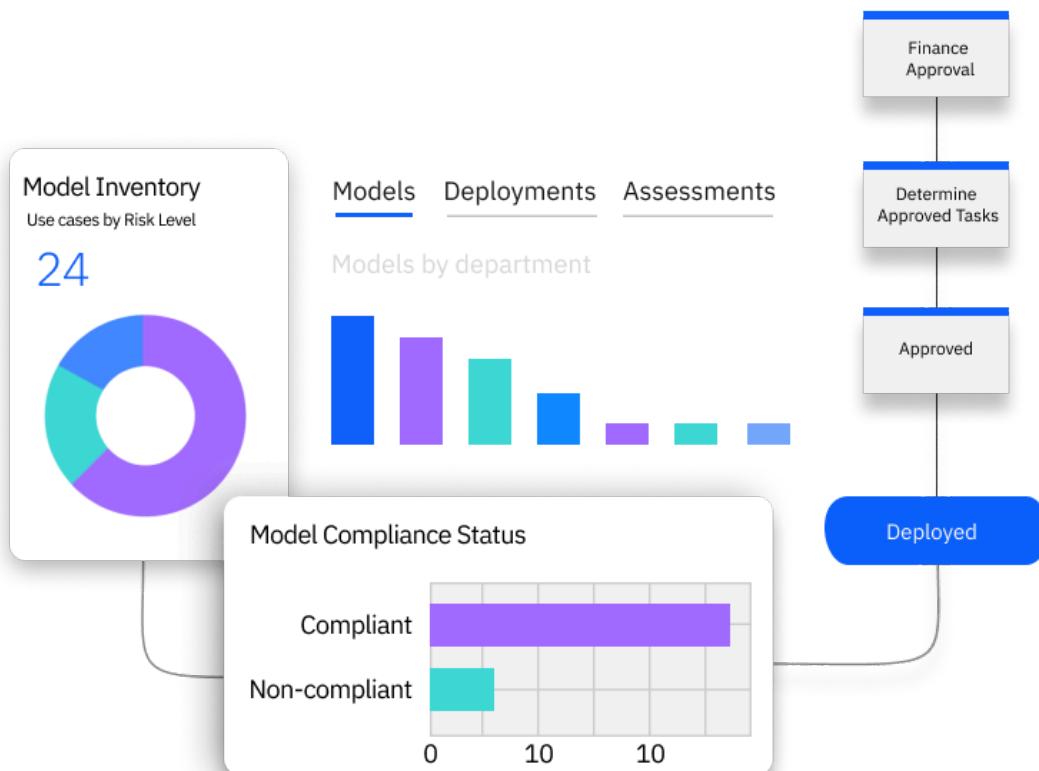


# Monitor and Govern AI with watsonx.governance Day 2

## Hands-on Lab Guide



Eric Martens  
emartens@ibm.com

# Contents

1. Introduction
2. Customize views
  1. Switch contexts
  2. Launch the governance console
  3. Create a business entity
  4. Create a custom field for the use case view
  5. Add the custom field to the use case view
  6. Disable the old view
3. Create a questionnaire template and custom workflow
  1. Create the questionnaire template
  2. Add questions
  3. Add the questionnaire to the existing AI assessments
  4. Update the AI assessment workflow
  5. Create workflow stages and actions
  6. Add resolution actions
  7. Update the stakeholder review workflow
4. Choose a lab to focus on
5. Govern generative models
  1. Create a model use case
  2. Progress the use case to the next phase
  3. Create the prompt template
  4. Track the prompt in the use case
  5. Deploy the model to a space
  6. Evaluate the model
  7. View the metrics in the governance console
6. Govern predictive models
  1. Create a predictive model use case
  2. Progress the predictive model use case to the next phase
  3. Open the watsonx monitoring dashboard
  4. Add the SageMaker model to the dashboard
  5. Configure the SageMaker monitors
  6. Configure explainability and fairness
  7. Configure quality and drift
  8. Evaluate the SageMaker model
  9. Link the SageMaker model to the use case
  10. View the model metrics in the use case
7. Conclusion

# 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

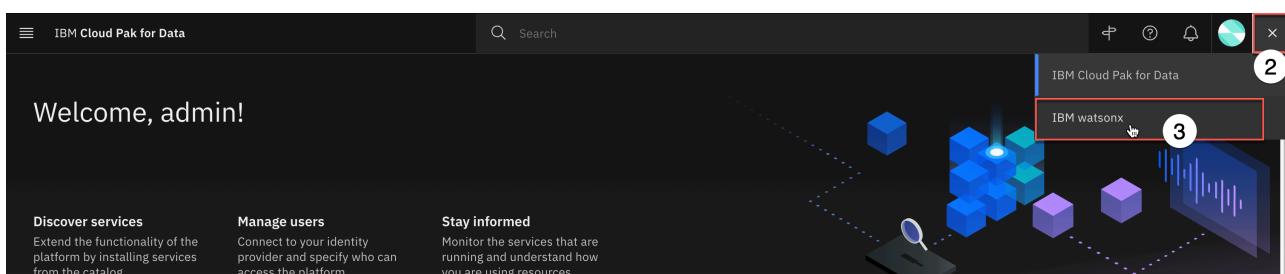
learning initiatives. In the context of watsonx.governance, the OpenPages solution is referred to as the [governance console](#). However, in many locations in the user interface, you will see it being referred to as OpenPages.

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.

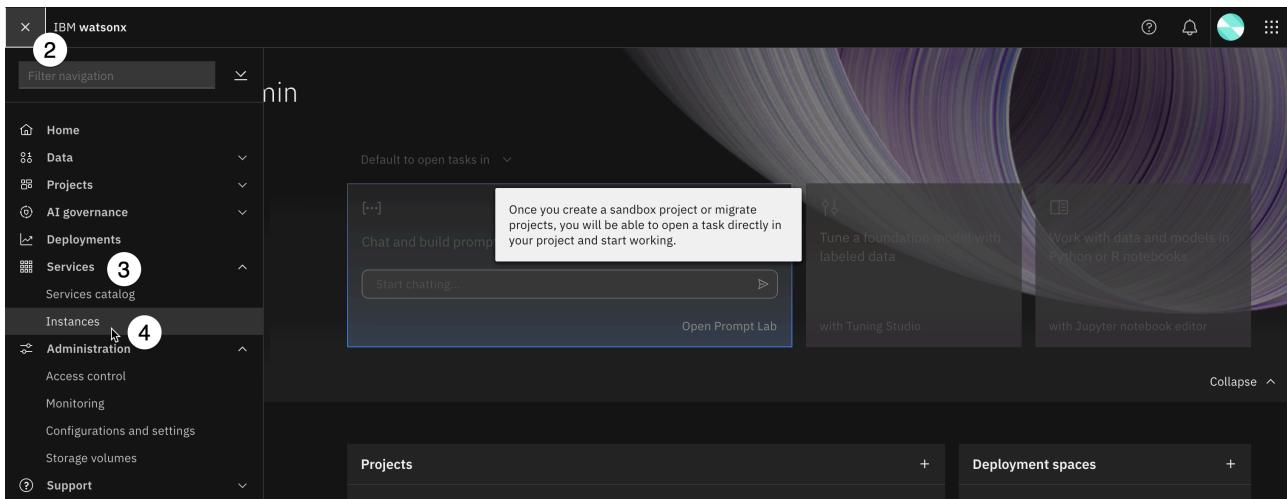
Your screen should now show IBM watsonx branding. This screen will be referred to throughout the lab as the watsonx home screen.

**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.

Name	Type	Created by	vCPU requests	Memory requests (GiB)	Data plane	Physical location	Status	Created on
cpd-database	db2oltp	admin	2.10	4.25 Gi	—	—	<span>green</span>	Oct 11, 2024
openscale-defaultinstance	aios	admin	0.00	0.00 Gi	—	—	<span>green</span>	Oct 8, 2024
<a href="#">openpagesinstance-cr</a>	openpages	admin	4.45	12.40 Gi	—	—	<span>green</span>	Oct 8, 2024

A callout box labeled '5' points to the 'openpagesinstance-cr' link in the Name column of the third row. Another callout box labeled '6' points to the 'Launch OpenPages' button in the Access information section of the instance details page.

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

The screenshot shows the details of the 'openpagesinstance-cr' instance. It includes sections for Status (Running), Database configuration, Access information, and Size. In the Access information section, there is a URL field containing a complex IBM Cloud URL. To its right is a 'Launch OpenPages' button, which is highlighted with a callout box labeled '6'. Below the URL field, there are fields for Database type (Internal database), Use dedicated nodes (True), and Node label (Node 1). The Size section shows a Data storage class of 'ocs-storagecluster-ceph-rbd'.

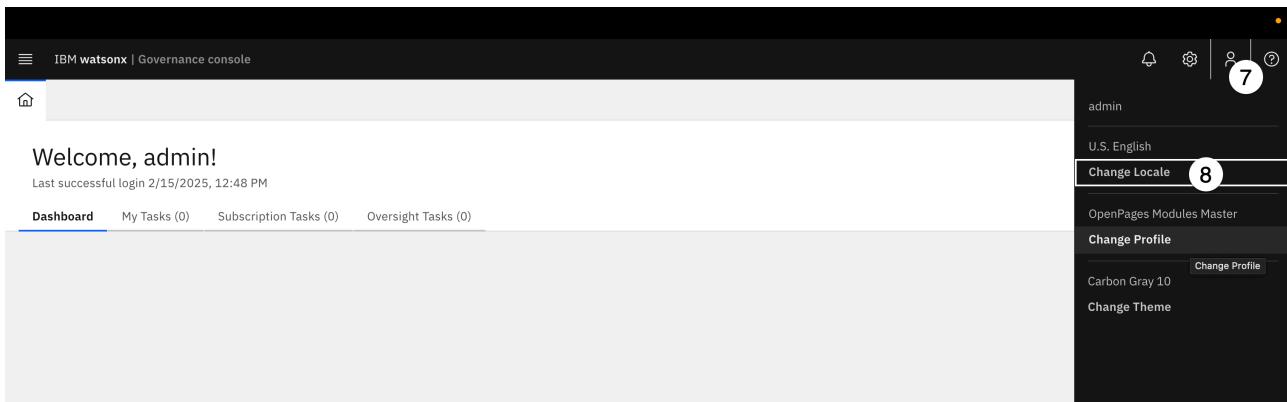
The OpenPages service launches in a new browser tab.

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).

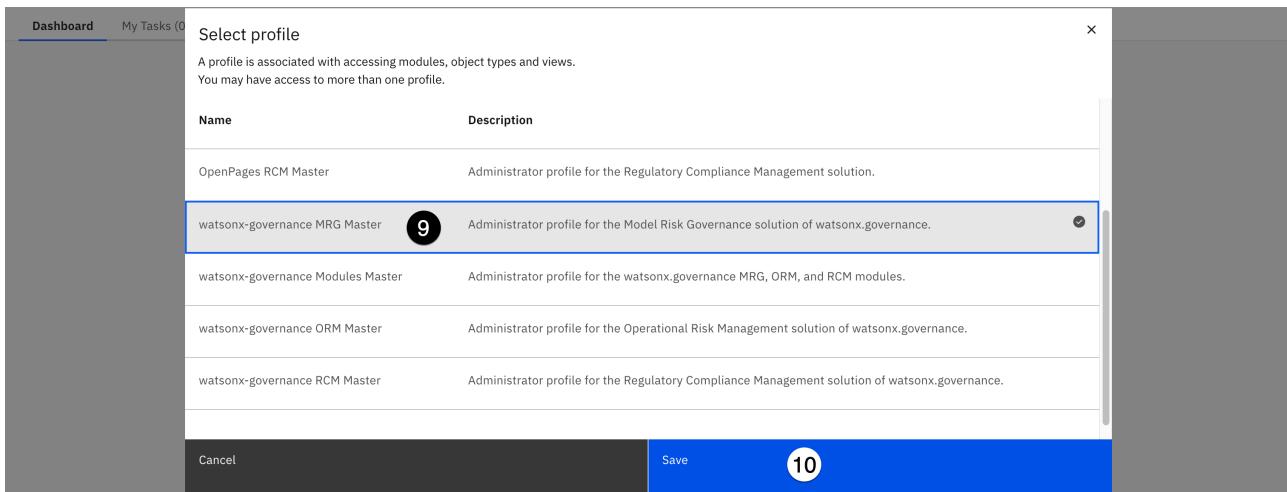
7. Click on the **avatar icon** in the upper left to open the user menu.

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.

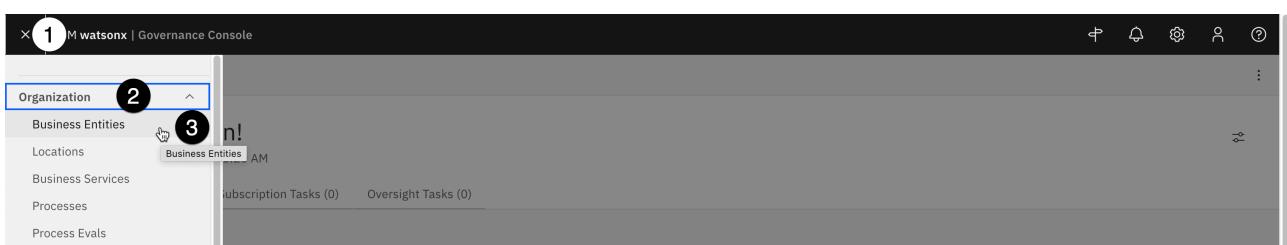


Your home screen should change, showing a variety of graphs on your dashboard.

### 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)

Name	Description	Executive Owner	Risk Appetite	In Scope	In RCSA Scope	Tags
<b>High Oaks Bank</b>	A global financial institution with operations across every continent, offering a broad range of financial services, including personal banking, credit cards, mortgages, auto financing, investment advice, small business loans, and payment processing.	admin	No			

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.

Name	Description	Tags
<b>Finance</b>	Worldwide corporate finance business unit	
<b>Human Resources</b>	Worldwide human resources business unit	

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.

The screenshot shows the 'Child Business Entity' table within the governance console. The table has columns for 'Name', 'Description', and 'Tags'. A blue button labeled 'New Business Entity' is highlighted with a circled number '10' above it. To the right, a modal window titled 'Create new Business Entity' is open, showing a progress bar at 100% completion and a message stating 'All Key Items (1)'. The 'Name' field is the only one completed, indicated by a green bar.

11. Enter [Regulatory Compliance](#) in the [Name](#) field.

The screenshot shows the 'Create new Business Entity' dialog. The 'Name' field is populated with 'Regulatory Compliance', which is circled with a number '11'. The 'Description' field is empty. On the right, a progress bar shows 'All Key Items (1)' completed, and the status bar indicates 'Name \*' is filled.

12. Enter [admin](#) in the [Executive Owner](#) field.

The screenshot shows the 'New Business Entity' dialog. The 'Executive Owner' field is populated with 'admin', which is circled with a number '12'. The 'Search users' button is visible below the field. On the right, a progress bar shows 'All Key Items (1)' completed, and the status bar indicates 'Name \*' is filled.

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.

The screenshot shows the IBM watsonx Governance console interface. At the top, there's a navigation bar with tabs for 'Business Ent...', 'High Oaks B...', 'Corporate', and 'Human Reso...'. On the far right of the header is a gear icon with a number '1' over it, which opens the Administration menu. The main content area displays a list titled 'Business Entities (56)' with columns for 'Name' and 'Description'. Several entities are listed, including 'AI Risk Library', 'Africa and Middle East', 'Asia', and 'Catalogs'. To the right of the list is the expanded Administration menu. A sub-menu under 'System Configuration' is shown, with 'Enable System Admin Mode' highlighted and a checkmark icon. A tooltip 'System Admin Mode: Disabled' is visible above the menu item. A callout bubble with the number '2' points to the 'Enable System Admin Mode' button.

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.

The screenshot shows the IBM watsonx Governance console interface. The top navigation bar has tabs for 'Business Ent...', 'High Oaks B...', and 'Corporate'. The gear icon in the header has a number '4' over it, opening the Administration menu. The main content area shows the 'Business Entities (56)' list. To the right is the expanded 'Solution Configuration' menu. The 'Object Types' item is highlighted with a checkmark icon and a number '5' over it. A callout bubble with the number '6' points to the 'Object Types' menu item. Below the menu, the 'Object Types' tab is active, showing a list of object types: Dashboards, Views, Workflows, Calculations, Scheduler, Object Types (which is the current tab), Profiles, Solutions, Tags, Themes, and Regulatory Event Rules.

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.

### Object Types (128)

Label	Name	Description
Use Case	Register	Unified Object Type
Use Case Review	UseCaseReview	Unified Object Type

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.

The screenshot shows the 'Fields' section of the 'Use Case' panel. At the top right, there is a 'New Field' button with a plus sign (circled with number 10). Below it, there is a dropdown menu labeled 'Field Groups' with 'Fields' selected (circled with number 9).

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.

The screenshot shows the 'New Field' panel with the 'General' tab selected. In the center, there is a 'Field Group' dropdown (circled with number 11) and a 'Name' input field. On the left side, there is a sidebar with various configuration options for the use case, including 'Label', 'Plural Label', and 'Global Search'.

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.

The screenshot shows the 'General' settings panel for an object. On the left, there's a sidebar with sections like 'Name', 'Description', 'Label', and 'Fields'. The 'Fields' section is expanded, showing fields such as 'Name' (set to 'Secondary EU AI Review'), 'Label' (empty), 'Description' (empty), and 'Data Type' (set to 'Enumerated String'). A callout bubble labeled '13' points to the 'Name' field. A callout bubble labeled '14' points to the 'Data Type' dropdown menu.

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.

The screenshot shows the 'New Field' panel under 'EU Compliance / New Field'. It has sections for 'General' (with 'Name' set to 'None'), 'Color Palette' (empty), 'Color Values' (empty), and 'Default Value' (empty). The 'Enumerated String Values' section is expanded, showing a list with 'None' and a 'New Value' button. A callout bubble labeled '15' points to the 'New Value' button.

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.

The screenshot shows the 'Fields' section of the 'Use Case' configuration. A new field named 'Funding Approved' is being created. The 'Data Type' is set to 'Enumerated String' with three color-coded options: 'Approved' (green), 'Denied' (red), and 'N/A' (yellow). The 'Required' checkbox is checked. The 'Create' button is highlighted with a blue border and a circled number 19.

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

An error message is displayed: 'Field Definition 'Secondary EU AI Review' already exists'. The timestamp is 2024-05-17 18:07:55.384. The 'New Field' panel is visible at the bottom right.

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.

The 'Administration' menu is open, showing various options like 'Solution Configuration', 'Users and Security', and 'System Admin Mode'. The 'System Admin Mode' option is highlighted with a circled number 21, and the 'Disable System Admin Mode' link is visible.

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.

Purpose	Description	Owner	Status	Risk Level	Tags
on	Uses internal and external recovery data, adjusted for macro-economic impact. Uses statistical regression	Bob Eldridge	Approved for Development	Low	
te bond - income	ALM based income forecast for the HTM portfolio, initially for the CCAR 2013 stress-test. Vendor solution	Bob Eldridge	Approved for Development	Medium	

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.

The screenshot shows the administration menu for the 'Agency Based LGD Estimation' use case. The 'Other' menu item is expanded, showing options like 'Background Processes', 'Logs', and 'Display Debug Info'. The 'Display Debug Info' option is highlighted with a blue border and a circled '7'.

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.

The screenshot shows a view titled 'Agency Based LGD Estimation'. At the top, there are tabs for 'Status' (Approved for Development), 'Risk Level' (Low), and 'Action'. A warning message in the top right corner states: 'This is a read-only system view and cannot be changed.' There are sections for 'General' and 'Tags'.

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.

The screenshot shows the 'New View' panel with the 'Copy view' button highlighted. The JSON preview shows a snippet of configuration code for a task use case.

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.

The screenshot shows the 'New View' panel with the 'Name' field set to 'custom-watsonx-Task-Register' and the 'Label' field also set to 'custom-watsonx-Task-Register'. The JSON preview shows the expanded configuration code.

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.

The screenshot shows the 'New View' panel with the 'Create' button highlighted. The 'Use as default view for all profiles' checkbox is checked. The JSON preview shows the full configuration code.

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.

The screenshot shows the WatsonX Task Register interface. At the top, there are buttons for 'View - Use Case', 'custom-watsonx-Task-Register', 'Type: Task', 'State: Draft', 'Copy view', 'Discard Draft', and 'Publish'. Below these are tabs for 'Design', 'JSON', and 'Preview', with 'Design' selected. On the left, a sidebar lists fields: Documentation, External ID, Inventory Name, LMID, Last Update, Secondary EU AI Review (with a red arrow pointing to it), Stakeholder Approval Completion Date, WKC Creation Date, and WKC Description. The main center panel shows the 'Regulatory Information' section, which contains 'Columns-0004' and 'EU AI Risk Category'. Below this is the 'Applicability Assessment Completion Date' item. A red arrow points from the 'Object Fields' list on the left to the 'Regulatory Information' section on the right. Number 13 is in a circle above the 'Regulatory Information' section, and number 14 is in a circle below it.

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.

The screenshot shows the WatsonX Task Register interface. On the left, a sidebar lists items: Card, Chart, Count, Grid (with a red arrow pointing to it), Tree, Object Fields, and Additional Information. The main center panel shows the 'Use Case Details' section, which contains 'Third Party Link', 'Section Fields', and 'Columns-0002'. The 'Columns-0002' section includes 'Uses Foundation Models' and 'Externally Facing'. To the right, a panel titled 'Use Case Approvals' is open, showing 'Edit' and 'Initially Collapsed' (set to False). Number 17 is in a circle above the 'Use Case Details' section.

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.

Published	Enabled	Default	System
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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)

Views (4)								
Label	Description	Object Type	View Type	Priority	Published	Enabled	Default	System
<input checked="" type="checkbox"/> watsonx-governance-Task-Register	Use Case (Register)	Task	3	✓	✓	✗	✓	✓
<input type="checkbox"/> watsonx-governance-Admin-Register	Use Case (Register)	Admin	2	✓	✓	✗	✓	✓
<input type="checkbox"/> watsonx-governance-New-Register	Use Case (Register)	Creation	3	✓	✓	✗	✓	✓
<input type="checkbox"/> custom-watsonx-Task-Register	Use Case (Register)	Task	1	✓	✓	✓	✗	✓

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.

The screenshot shows the WatsonX Governance console interface. The top navigation bar includes links for IBM WatsonX, High Oaks B..., Corporate, Object Types, Conversations, Workflows, AI Assessments, Use Case Requests, and Help. On the left, a sidebar menu is expanded under the 'Assessments' tab, showing options like Risks, Controls, Questionnaire Templates (which is highlighted with a black circle), and others. The main content area displays four cards: 'Change Management' (41 Change Requests by Status), 'Model Inventory' (33 Use Cases by Risk Level), and 'Use Cases by Lifecycle Phase' (33 total, with a pie chart showing distribution). The 'Questionnaire Templates' card is also visible.

4. Click the **New** button in the upper right.

The screenshot shows the 'Questionnaire Templates (1)' section of the IBM Watson Governance console. At the top, there are navigation tabs: Object Types, Use Case, Use Cases, Agency Base..., and Questionnaire... (which is selected). Below the tabs is a search bar and a table header with columns: Name, Description, Primary Owner, Type, Completion Required, and Tags. A single row is visible in the table, labeled 'AI Risk Identification Questionnaire'. In the top right corner of the interface, there is a 'New' button with a circled '4' over it, indicating the next step in the process.

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

6. Enter a description in the **Description** field.

This screenshot shows the 'New Questionnaire Template' dialog. On the left, there's a form with fields for Name (containing 'Secondary EU AI Act Review' with a circled '5'), Description (containing 'Second-level review to determine if the use case violates the EU AI Act.' with a circled '6'), and Rationale (empty). On the right, a validation summary window lists '2 items require attention': 'Name' and 'Description'. There are also dropdowns for 'All Key Items (5)', 'Primary Owner', and 'Folder'.

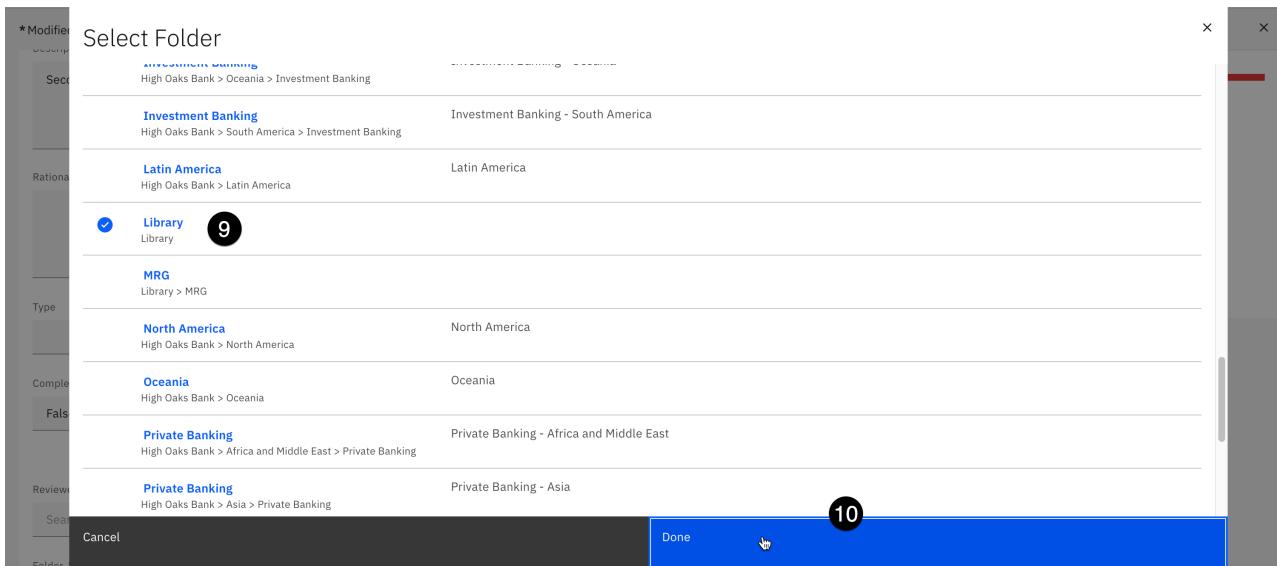
7. Enter the **admin** user in the **Primary Owner** field.

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

This screenshot shows the 'Select Folder' dialog. It includes fields for 'Type' (dropdown), 'Questionnaire Scoring Method' (dropdown set to 'Simple'), 'Completion Required' (dropdown set to 'False'), 'Primary Owner' (dropdown showing 'admin' with a circled '7'), 'Reviewer' (button 'Search users'), 'Approver' (button 'Search users'), and a 'Folder' dropdown. A large 'Select Folder' button at the bottom is circled with a '8'.

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.

Questionnaire Template  
Secondary EU AI Act Review ⚡ ☆ ^

Task   Activity   Admin   **Editor** 1

**Let's get started!**

Start by creating a new questionnaire template.

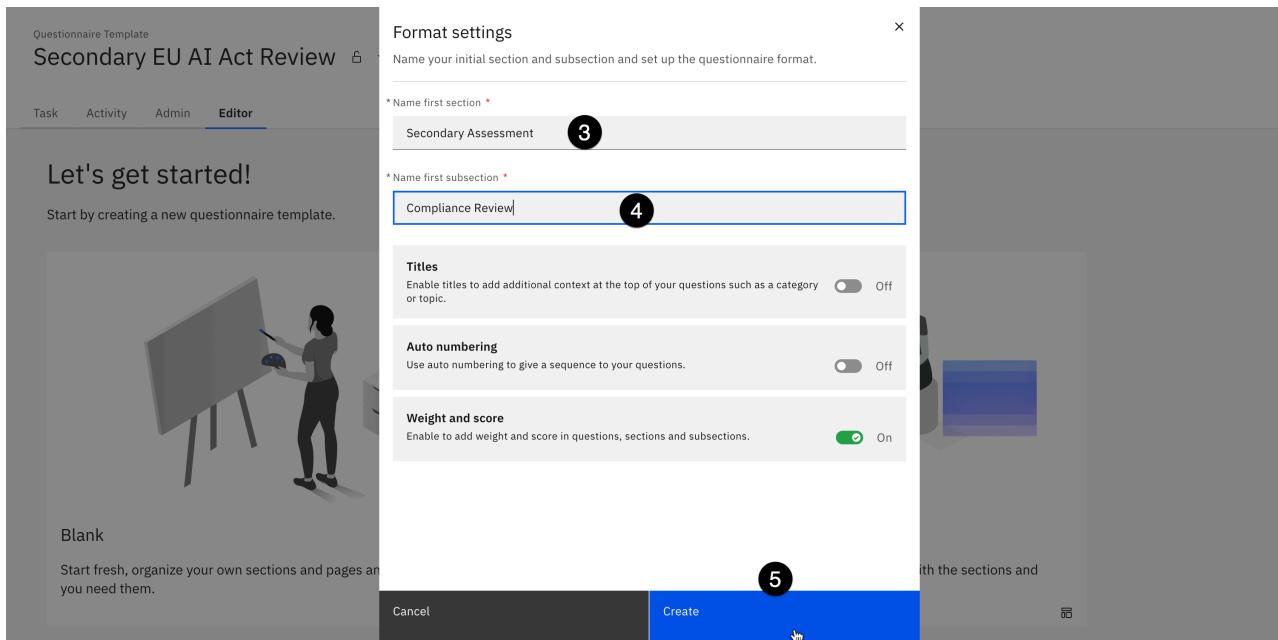
**Blank**

Start fresh, organize your own sections and pages and create new questions as you need them.

**From template**

Select from the list of available templates and start with the sections and questions you need.

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.

The screenshot shows the IBM Watsonx Governance console interface. On the left, there's a sidebar with navigation links like 'Business Ent...', 'High Oaks B...', 'Corporate', and 'Human Reso...'. The main area displays a list titled 'Business Entities (56)' with columns for 'Name' and 'Description'. Items listed include 'AI Risk Library', 'Africa and Middle East', 'Asia', and 'Catalogs'. On the right, a vertical 'Solution Configuration' menu is open, showing options like 'Users and Security', 'System Configuration', 'Integrations', 'System Migration', 'Other', 'FastMap Import', and 'Enable System Admin Mode'. A callout bubble labeled '1' points to the gear icon in the top right corner of the menu. Another callout bubble labeled '2' points to the 'Enable System Admin Mode' button, which is highlighted with a cursor icon.

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.

The screenshot shows the same interface as before, but now the 'Object Types' tab is active in the 'Solution Configuration' menu. The menu items visible are 'Dashboards', 'Views', 'Workflows', 'Calculations', 'Scheduler', 'Object Types' (which is highlighted with a cursor icon), 'Profiles', 'Solutions', 'Tags', 'Themes', and 'Regulatory Event Rules'. A callout bubble labeled '4' points to the gear icon in the top right corner of the menu. Another callout bubble labeled '5' points to the 'Object Types' menu item. A third callout bubble labeled '6' points to the 'Object Types' tab itself.

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

## Object Types (128)

Label	Name	Description
Questionnaire Assessment <span style="border: 1px solid black; border-radius: 50%; padding: 2px;">7</span>	QuestionnaireAssessment	OpenPages GRC Object Type

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.

Name	Label	Description	Data Type	Required	Global Search
AI Assessment Type	AI Assessment Type	AI Assessment Type	Enumerated String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

AI Assessment Type

Raise

Global Search

True

False

Hierarchical False

Enumerated String Values 10 [New Value](#) +

- [Not Determined](#)
- [Data Gathering](#)

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

New Enum Value

* Name *	Secondary EU Assessment
* Label *	Secondary EU Assessment

[Edit](#)

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.

The screenshot shows the IBM Watsonx Governance console interface. At the top, there's a navigation bar with tabs like 'Business Ent...', 'High Oaks B...', 'Corporate', 'Object Types', and 'Conversation...'. On the far right of the header is a gear icon (labeled 1) which opens the Administration menu. The main content area shows a 'Use Case' section for 'Conversational AI' with status 'Approved for Development' and risk level 'High'. Below this is a table with columns 'Task', 'Activity', and 'Admin'. The 'Task' column has a link to 'View Name : custom-watsonx-Task-Register'. Under 'Task', there's a note '\* Modified Required \*'. The 'Activity' and 'Admin' columns are empty. To the right of the table is a sidebar labeled 'Solution Configuration' (labeled 2) containing links for Dashboards, Views, Workflows (which is highlighted), Calculations, Scheduler, Object Types, Profiles, Solutions, and Tags. The 'Workflows' link leads to the 'Workflows' tab (labeled 3) where the 'AI Assessment Workflow' is listed.

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

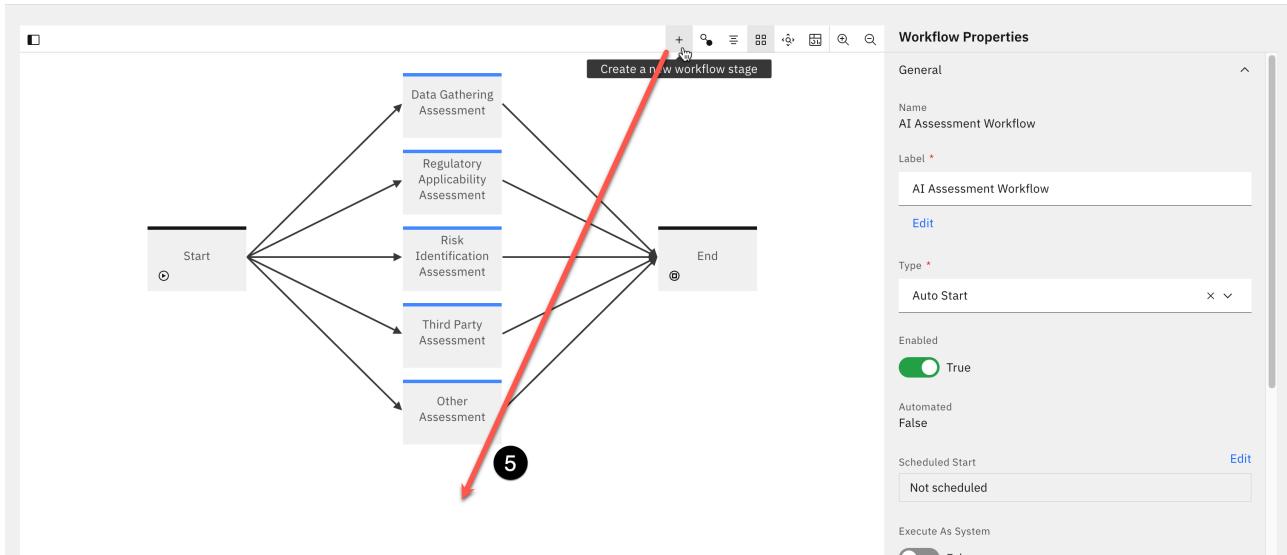
The screenshot shows the 'Workflows (41)' editor palette. It features a search bar at the top left and a 'New Workflow +' button at the top right. Below is a table with columns: Label, Name, Object Type, Version Number, Type, Automated, Published, and Enabled. The table lists several workflows:
 

Label	Name	Object Type	Version Number	Type	Automated	Published	Enabled
<input checked="" type="checkbox"/> <a href="#">AI Assessment Workflow</a>	AI Assessment Workflow	Questionnaire Assessment	1	Auto Start	✗	✓	✓
<input type="checkbox"/> <a href="#">Action Item Approval Workflow</a>	Action Item Approval Workflow	Action Item	1	Auto Start	✗	✓	✓
<input type="checkbox"/> <a href="#">FCM Certification - Business Level</a>	Business Level SOX Certification	Business Entity	1	Manual Start	✗	✓	✓
<input type="checkbox"/> <a href="#">Challenge</a>	Challenge	Challenge	1	Auto Start	✗	✓	✓

 The 'AI Assessment Workflow' row is selected, indicated by a blue highlight and a circled number 4 above the row. The 'New Workflow +' button is also circled with a number 4.

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.

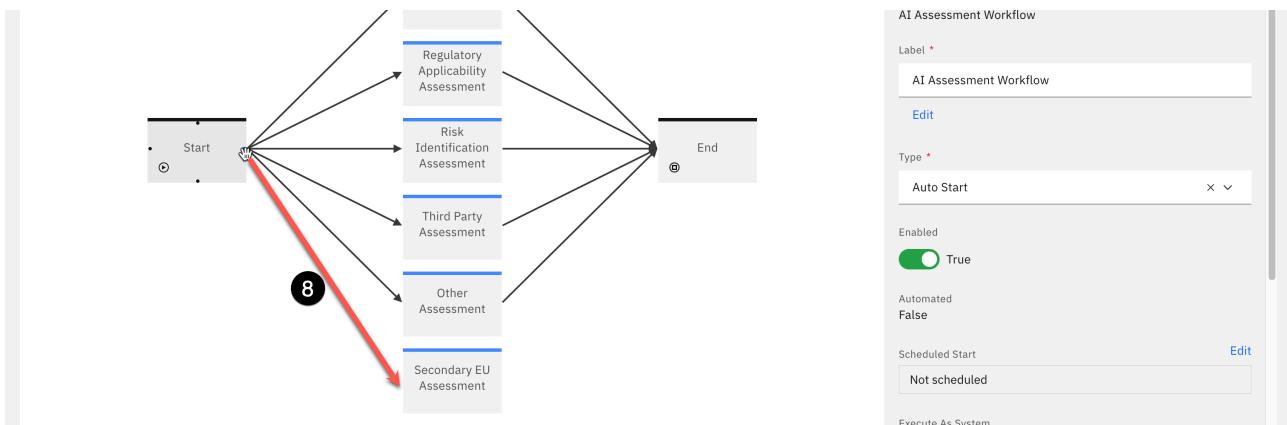


6. Enter **Secondary EU Assessment** in the **Name** field.

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

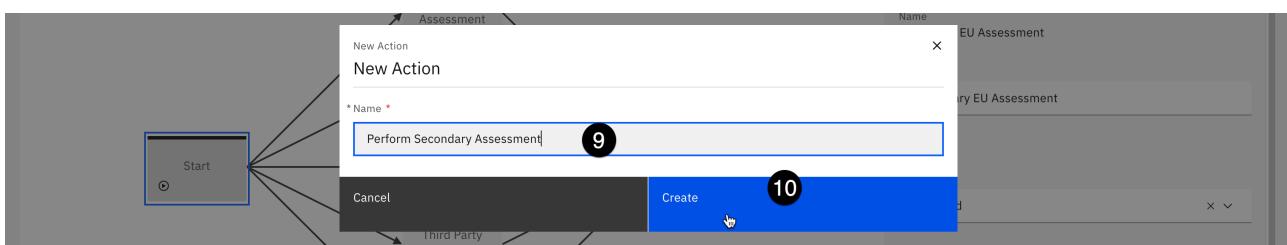


8. Hover your mouse pointer over the **Start** workflow stage to make four black boxes appear on the stage border. Click and drag one of the boxes to the new **Secondary EU Assessment** stage box to create an action linking the two stages. The **New Action** dialog opens.



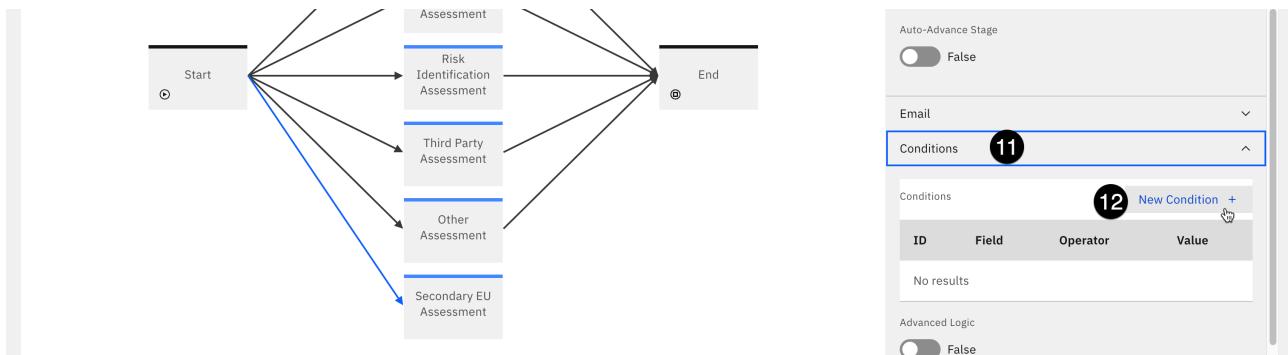
9. Enter **Perform Secondary Assessment** in the **Name** field.

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.

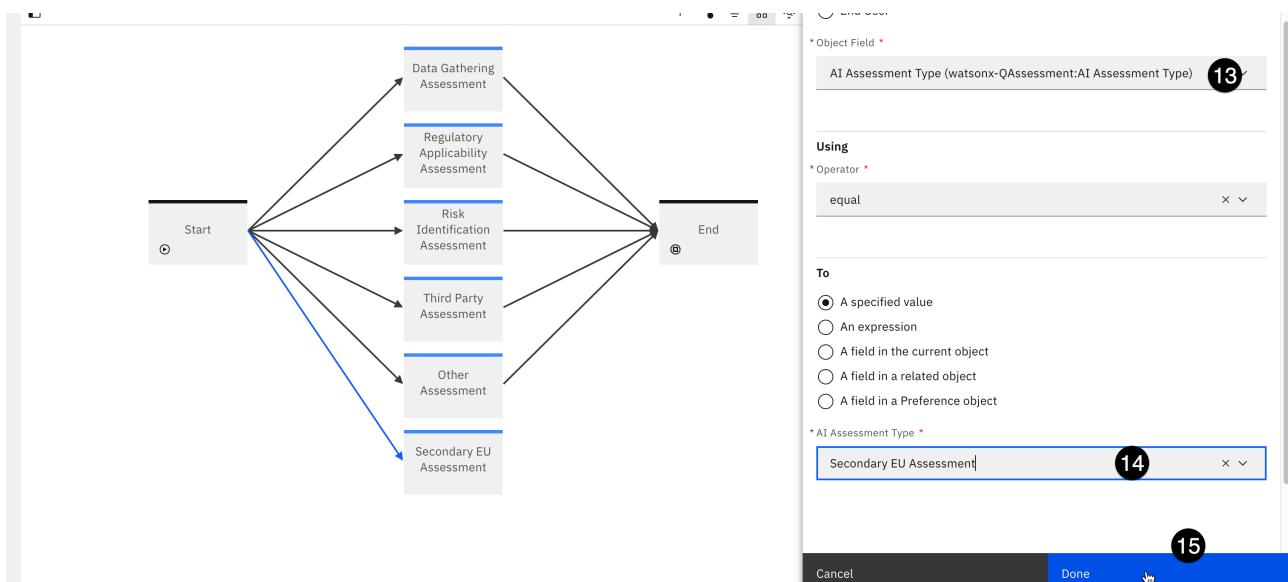
12. Click on the New Condition button. The Conditions panel opens.



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.

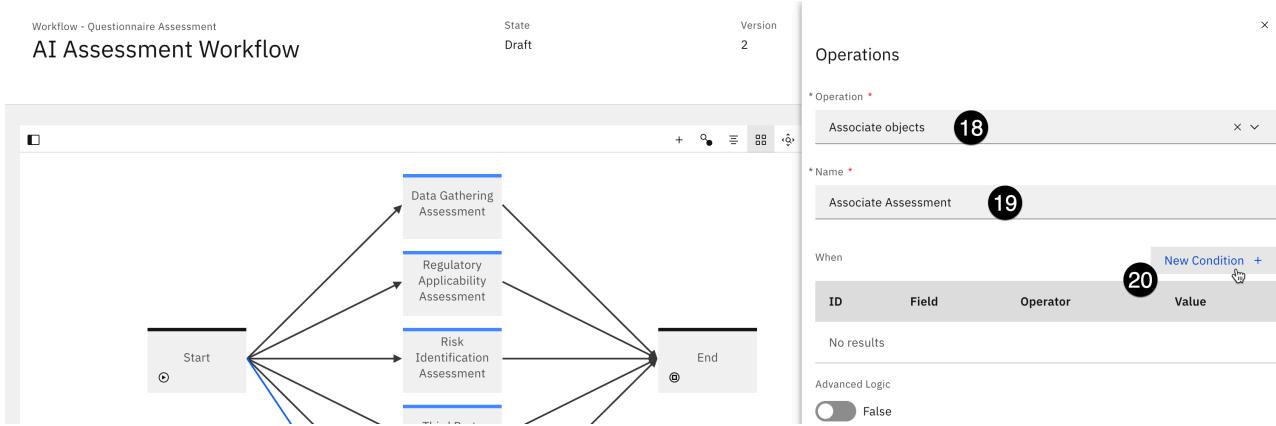
17. Click on the New Operation button. The Operations panel opens.



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.

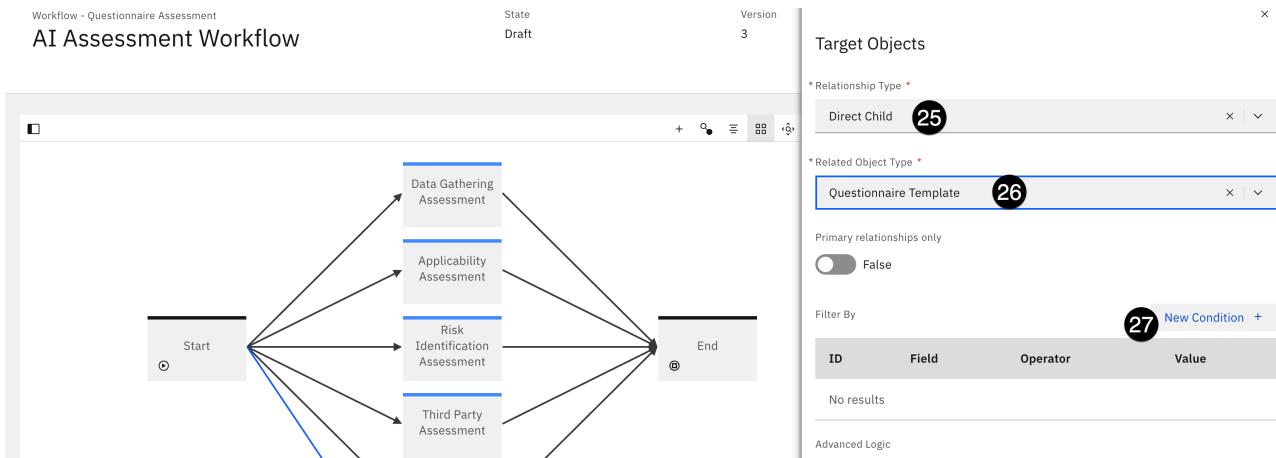
**Note:** In some versions of the software, **Target Objects** may be called **Objects to associate**.



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

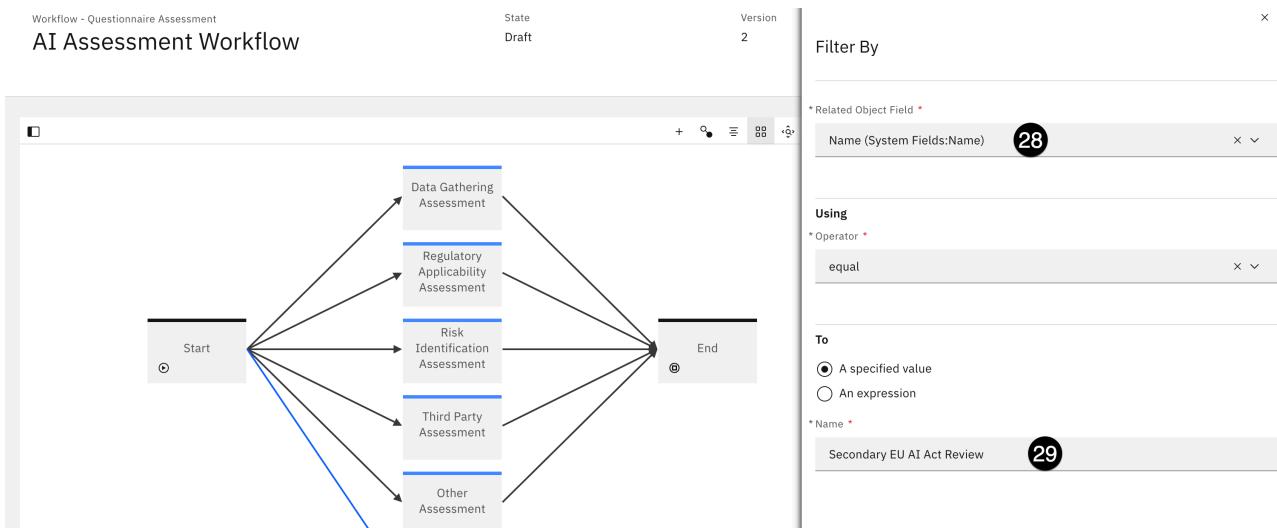
26. Click on the **Related Object Type** dropdown and select **Questionnaire Template** from the list.

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.

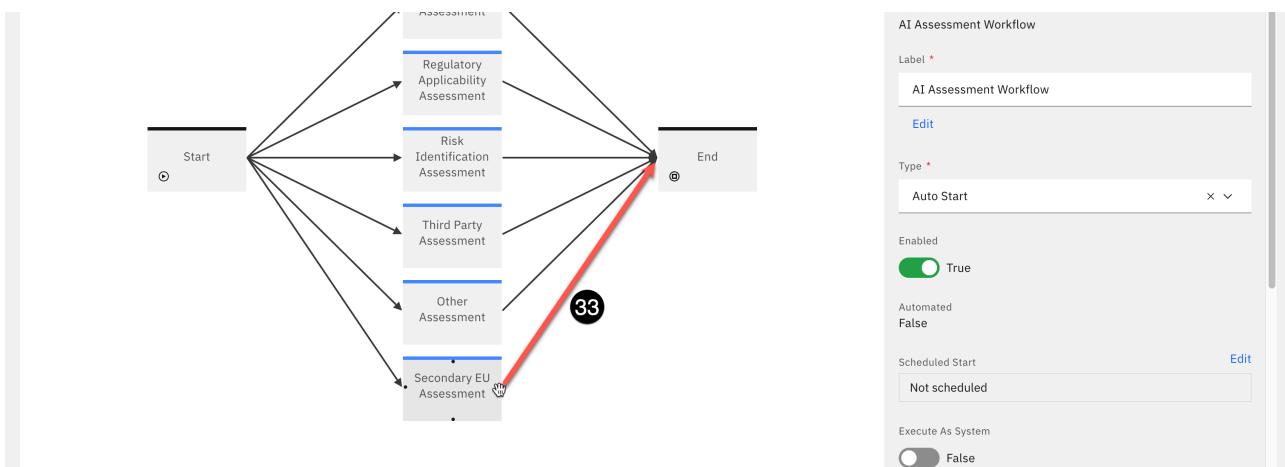
29. Enter the exact name of the questionnaire template you created in a previous step in the **Name** field.  
 If you have been following the instructions, you named it **Secondary EU AI Act Review**.



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.

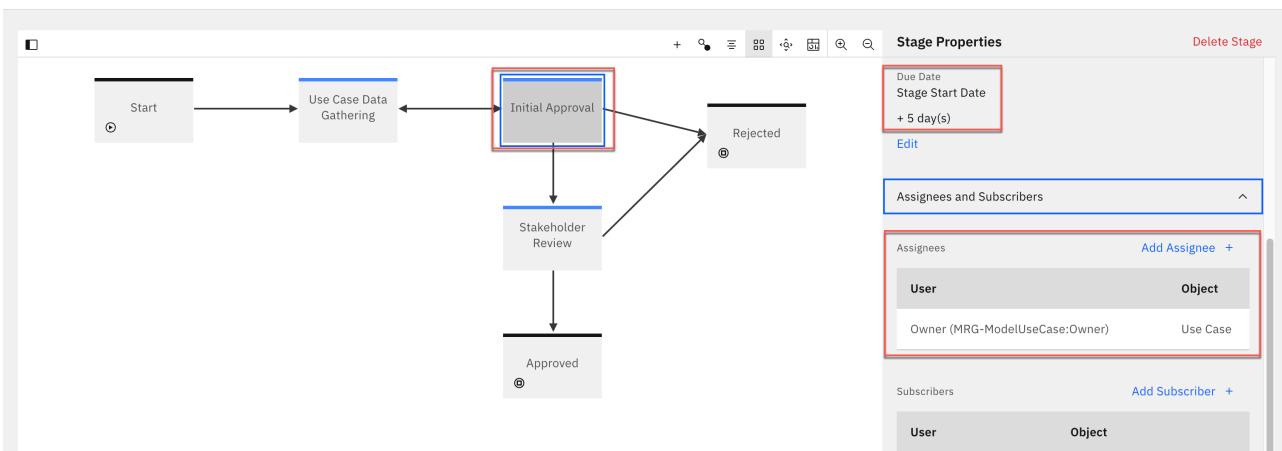
The screenshot shows the IBM Watsonx Governance console interface. At the top, there's a navigation bar with tabs like 'Business Ent...', 'High Oaks B...', 'Corporate', 'Object Types', and 'Conversation...'. On the far right of the header is a gear icon (labeled 1) which opens the 'Administration' window. Below the header, the main area has a dark sidebar on the right labeled 'Solution Configuration' with options like 'Dashboards', 'Views', 'Workflows' (which is highlighted and labeled 2), 'Calculations', 'Scheduler', 'Object Types', 'Profiles', 'Solutions', and 'Tags'. The main content area shows a table of workflows. One workflow is selected, 'Conversational AI', which is described as 'Approved for Development' with a 'High' risk level. The table includes columns for Task, Activity, Admin, Name, Use Case Type, and Status. A 'Tags' section on the right indicates 'No tags have been applied yet'.

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

The screenshot shows the 'Use Case Request' workflow editor palette. It displays a table of workflow stages. The 'Use Case Request' stage is highlighted with a large number 4 over it. The table columns include Stage, Action, Type, Count, Start Type, and several status indicators (X or checkmark). The 'Use Case Request' stage is listed as '1' with 'Auto Start'. Below the table, there are pagination controls: 'Items per page: 40' and '1-40 of 41 items'.

Stage	Action	Type	Count	Start Type			
Signature Revoke	Signature Revoke	Signature	1	Manual Start	X	✓	✓
Use Case Deployment Approval	Use Case Deployment Approval	Use Case	1	Manual Start	X	✓	✓
Use Case Development and Validation	Use Case Development and Validation	Use Case	1	Manual Start	X	✓	✓
<a href="#">Use Case Request</a> 4	Use Case Request	Use Case	1	Auto Start	X	✓	✓
Use Case Stakeholder Review	Use Case Stakeholder Review	Use Case Review	1	Auto Start	X	✓	✓
Vendor Identified Global Issue	Vendor Identified Global Issue	Issue	1	Manual Start	X	✓	✓

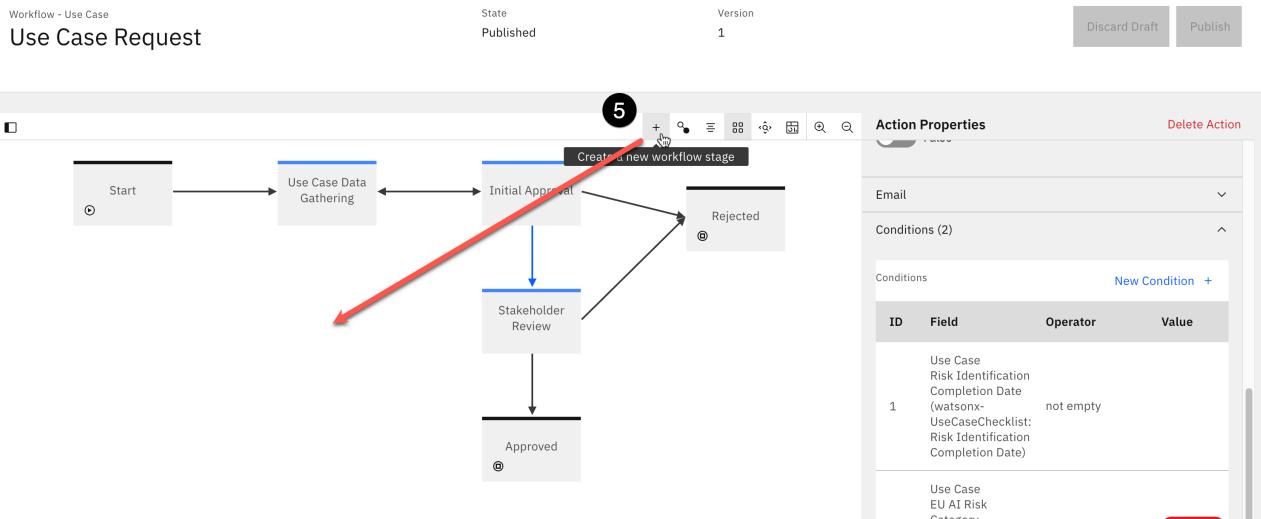
Take a moment to explore the items in the palette by clicking on them and observing the [Workflow Properties](#) panel on the right of the screen. For example, click on the [Initial Approval](#) box. Boxes represent stages of the workflow. In the properties panel, you can see that the due date of the 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.

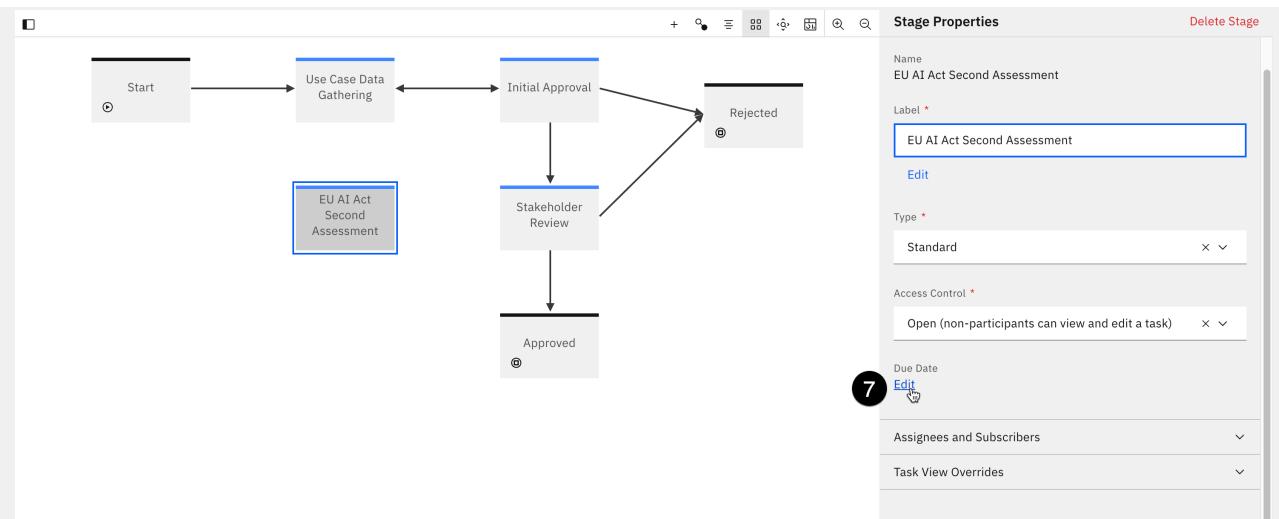
However, what if the organization wanted a second assessment in the case of a *Prohibited* result? In the steps below you will configure that as part of the workflow.

- 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.



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

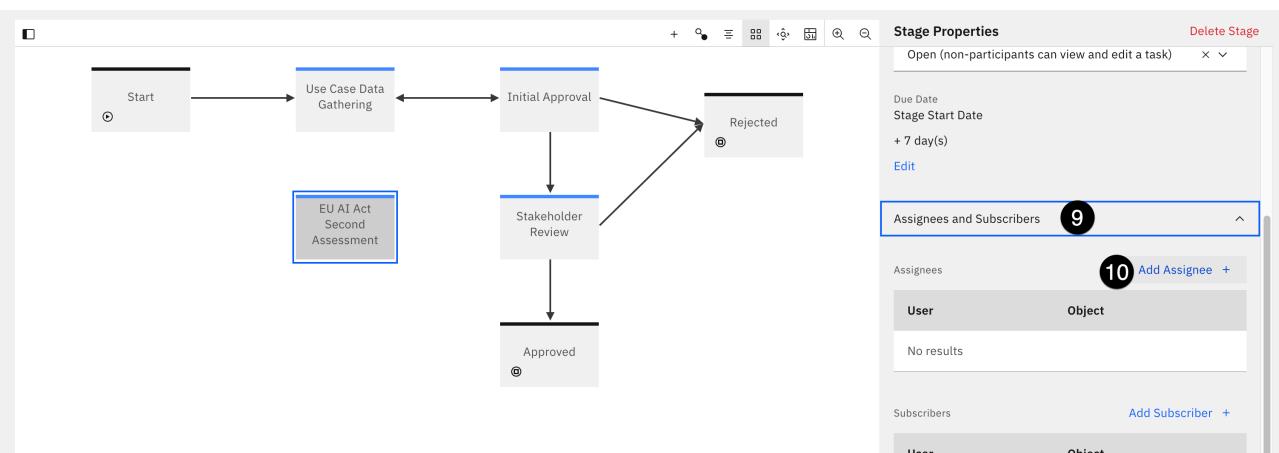
- In the **Stage Properties** panel, click the **Edit** button below the **Due Date**.



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.

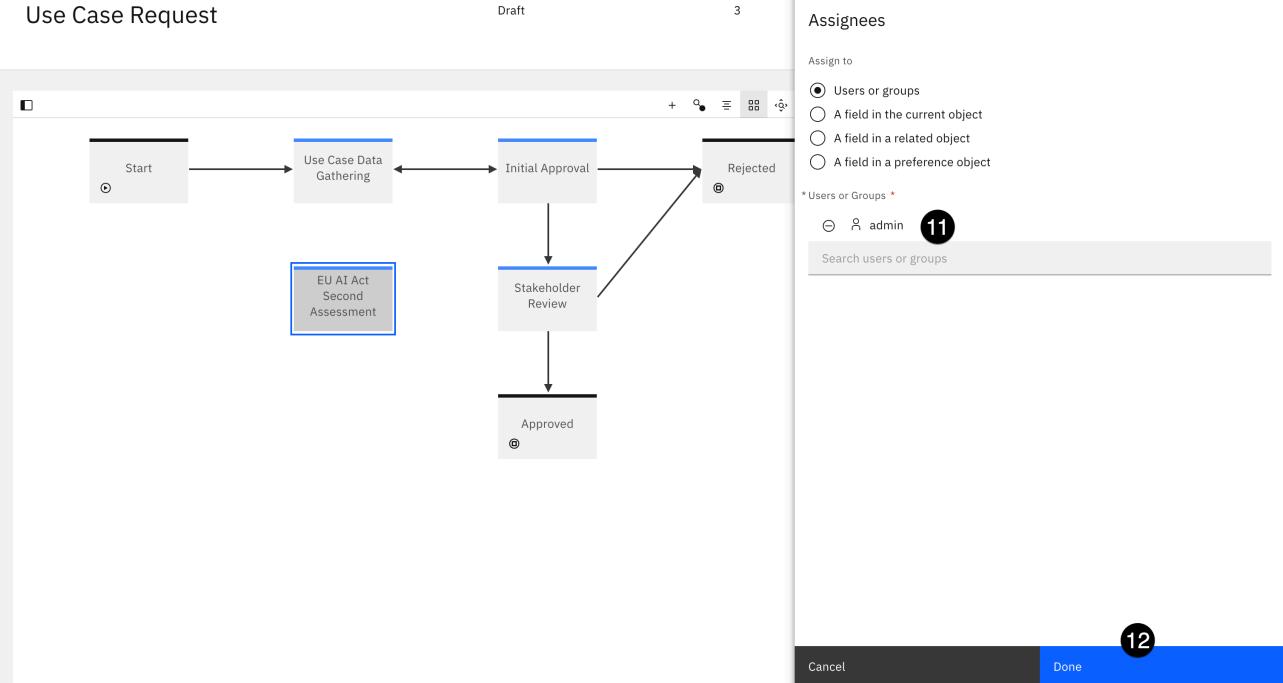
10. Click on the **Add Assignee** button. The **Assignees** panel opens.



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.

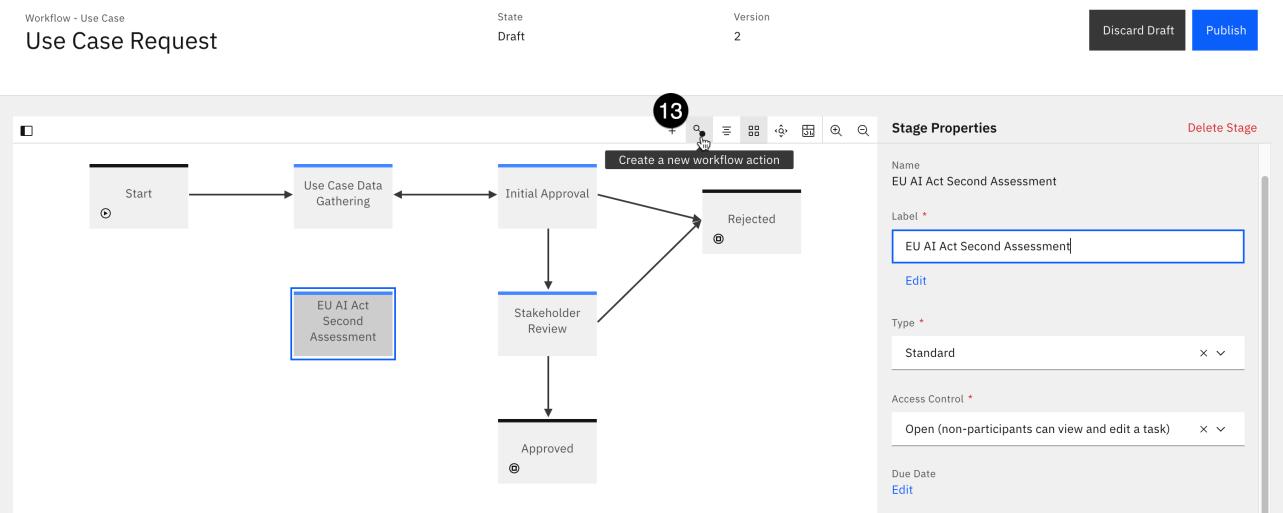
12. Click **Done**.

## Use Case Request



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

- 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.

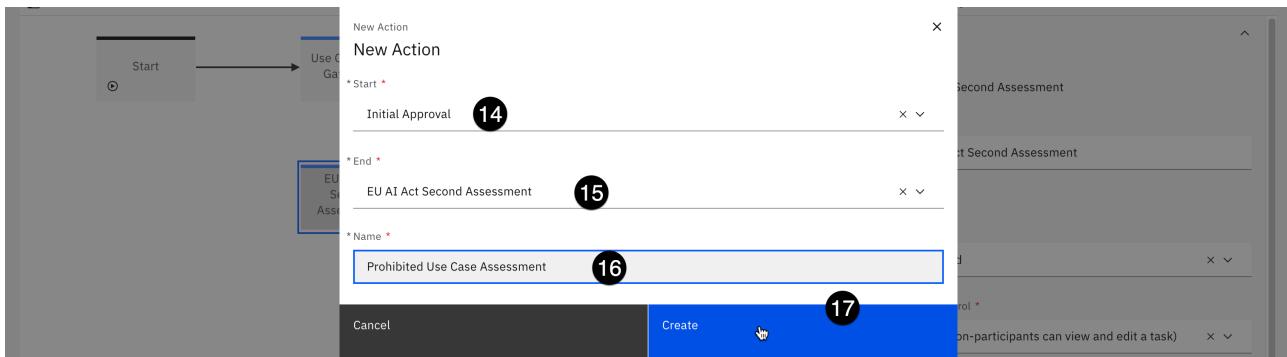


- Click the [Start](#) dropdown and select the [Initial Approval](#) stage.

- Click the [End](#) dropdown and select the [EU AI Act Second Assessment](#) stage you just created.

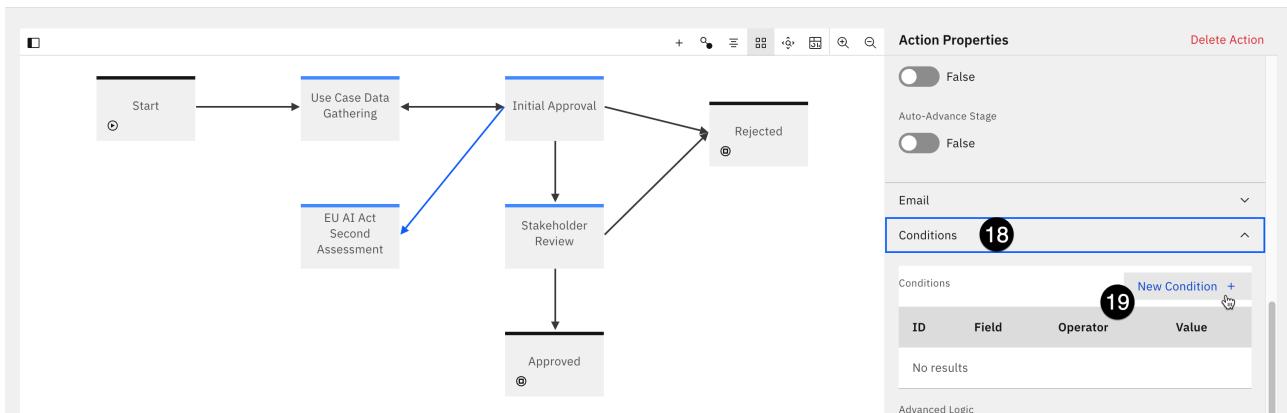
- Enter [Prohibited Use Case Assessment](#) in the [Name](#) field. The text you enter into this field will appear as an available action in the [Actions](#) menu in the model use case view when the use case is in this stage.

- 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.

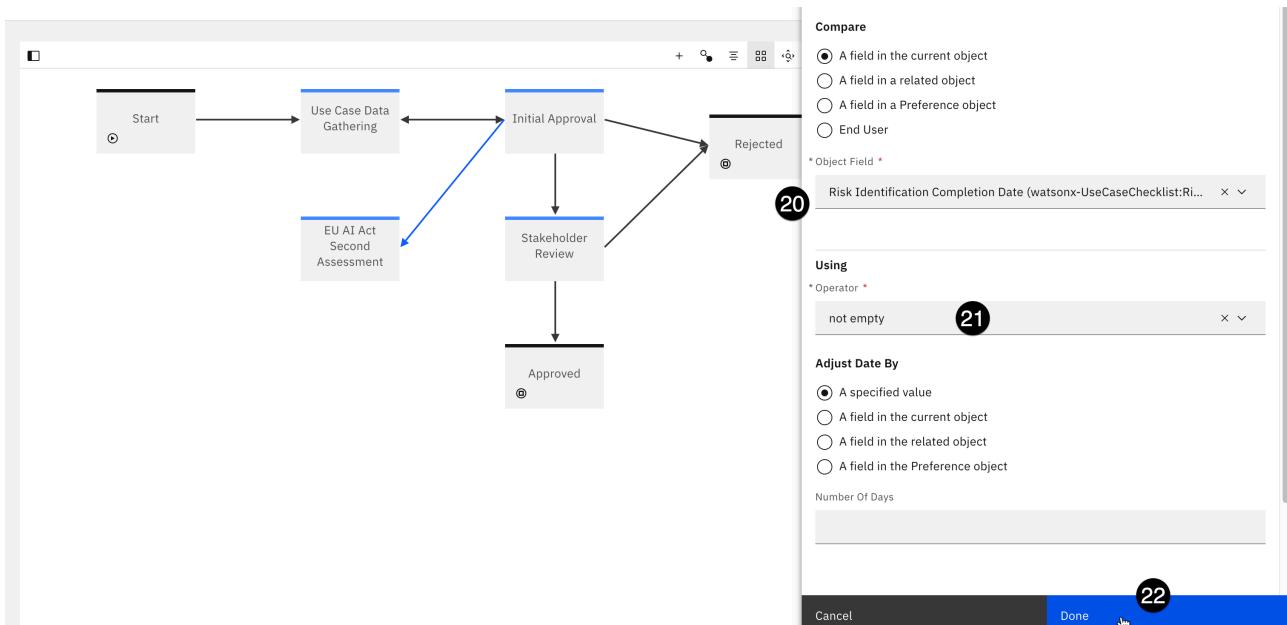
19. Click on the **New Condition** button. The **Conditions** panel opens.



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.



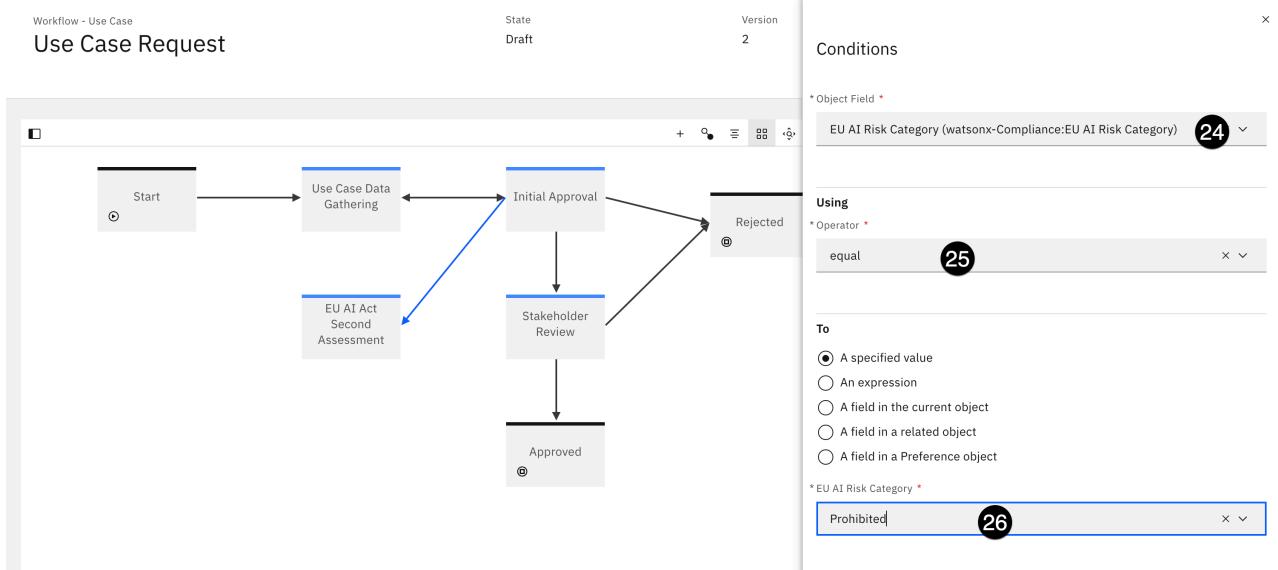
23. Click the **New Condition** button again to add a second condition.

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**.

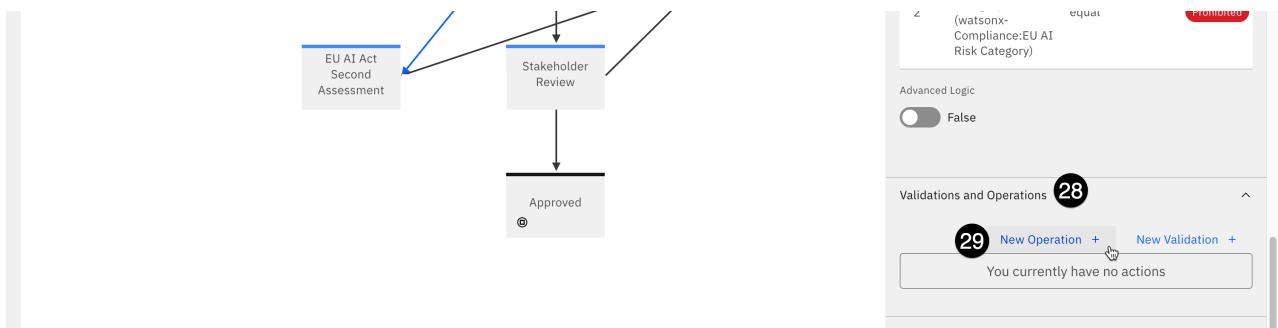
27. Click **Done** to add the condition.



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.

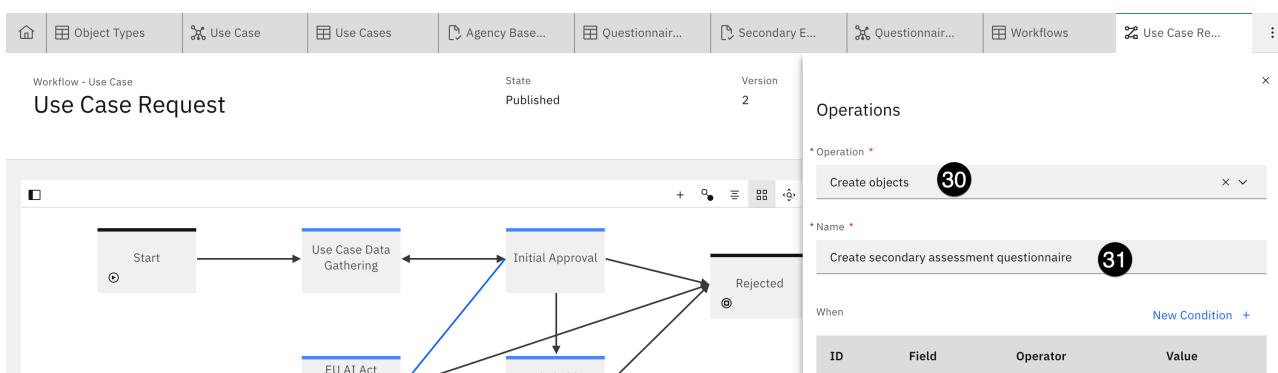
28. In the **Action Properties** panel, click on the **Validations and Operations** section to expand it.

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.

The screenshot shows the 'Fields' panel with a 'Related Object Type' dropdown set to 'Questionnaire Assessment'. A large arrow points down to the 'Approved' stage in the workflow diagram on the left.

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.

The screenshot shows the 'Workflow - Use Case Request' panel. The 'Fields' panel on the right has an 'Object Field' dropdown set to 'AI Assessment Type (watsonx-QAssessment:AI Assessment Type)'. Below it, an 'AI Assessment Type' dropdown is set to 'Secondary EU Assessment'. The main panel shows a workflow with stages: Start, Use Case Data Gathering, Initial Approval, Stakeholder Review, Approved, and Rejected. Transitions include a direct arrow from 'Initial Approval' to 'Rejected', and another from 'Initial Approval' to 'Stakeholder Review'. A blue arrow points from 'EU AI Act Second Assessment' to 'Rejected'.

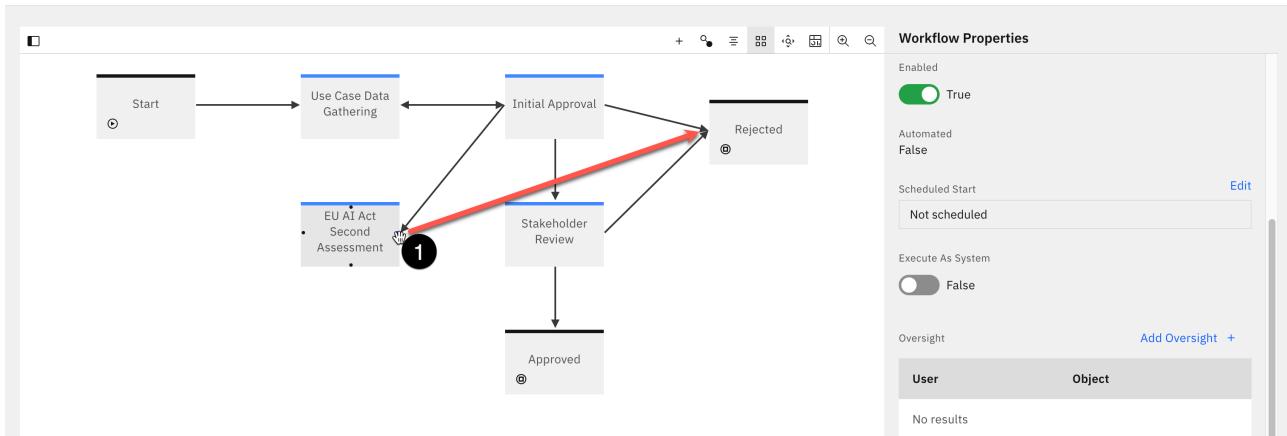
36. Click the [Done](#) button in the lower right to close the [Fields](#) panel.

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

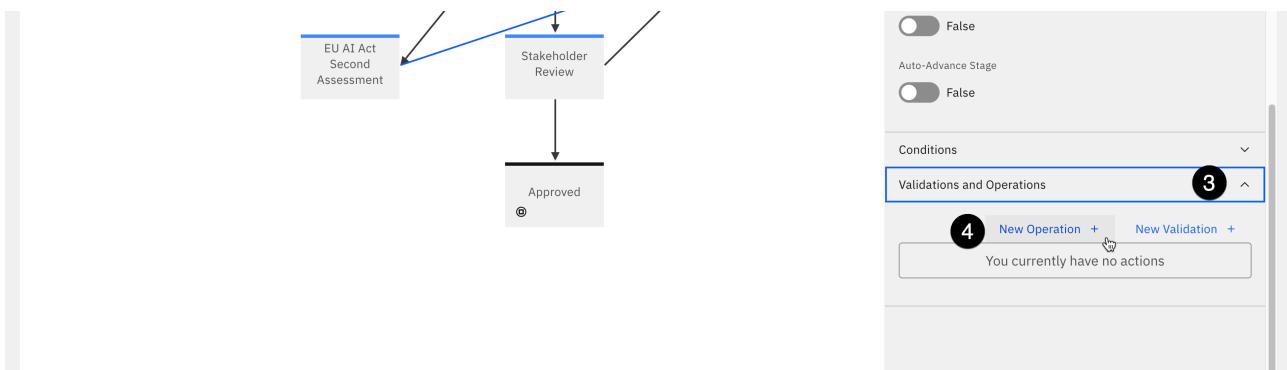
1. Hover your mouse over the [EU AI Act Second Assessment](#) stage; four black dots appear on the borders of the stage box. Click and drag one of the dots from the stage over to the [Rejected](#) stage on the palette to create an action linking the two. The [New Action](#) dialog appears.



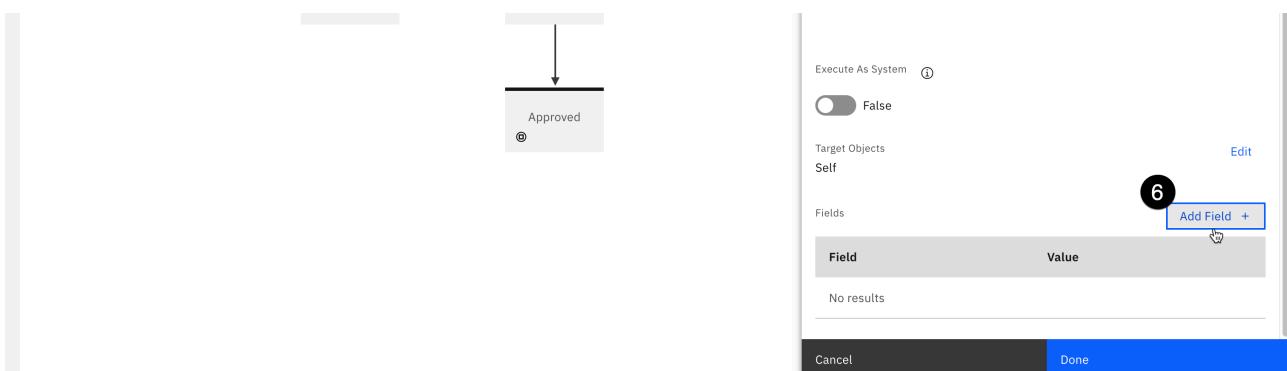
- Enter **Reject Use Case** in the **Name** field and click **Create**. This value is what will appear in the user interface for the stage owner for them to reject the use case.

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

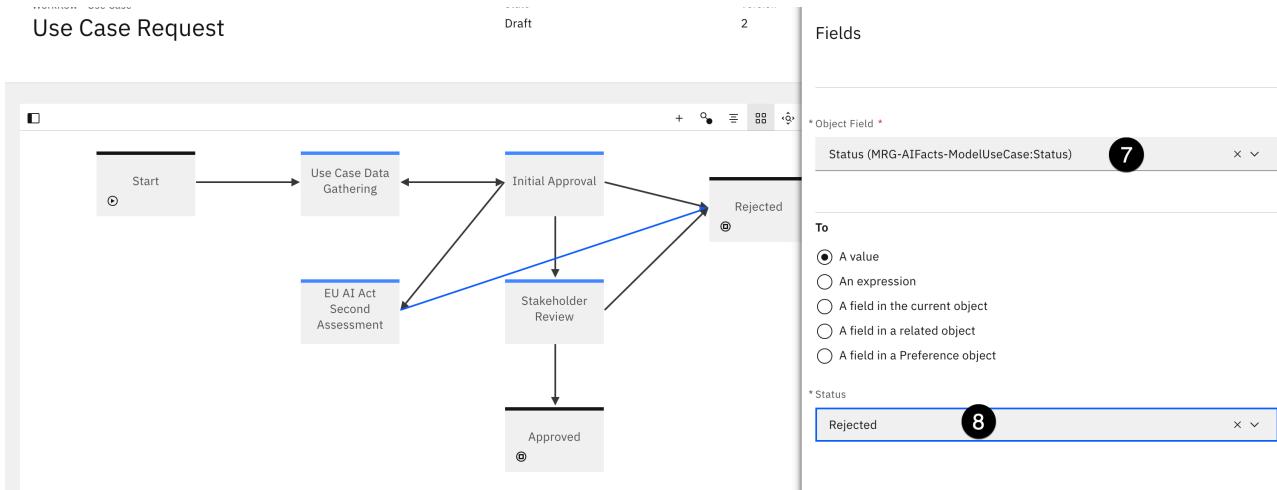
- In the **Action Properties** panel, scroll down the bottom and click on the **Validations and Operations** section to expand it.
- Click on **New Operation**. The **Operations** panel opens.



- Enter **Set status as rejected** in the **Name** field.
- Scroll to the bottom of the panel and click the **Add Field** button.



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

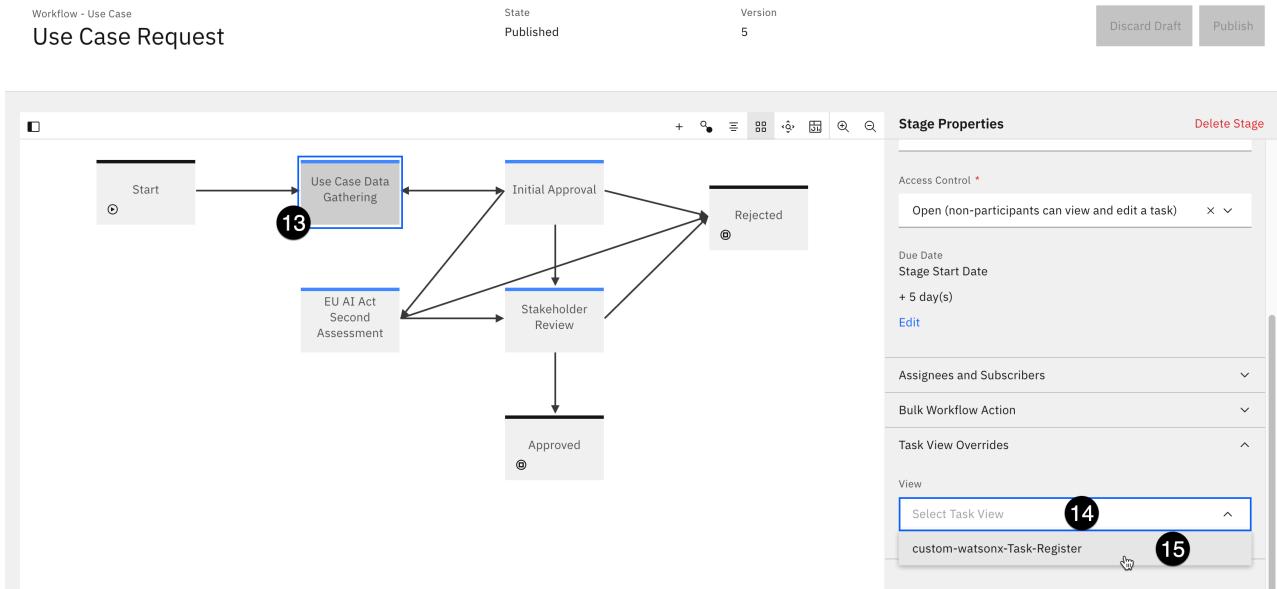


9. Click **Done** to create the field on the operation.
10. Click **Done** again to set the operation on the action. Performing the action will now update the model status.
11. Repeat step 1 above, clicking and dragging from the **EU AI Act Second Assessment** stage to the **Stakeholder Review** stage 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.

The screenshot shows the 'Workflows (1)' section of the IBM Watsonx Governance console. A single workflow, 'Use Case Stakeholder Review', is listed in the table. The table columns include Label, Name, Object Type, Version Number, Type, Automated, Published, and Enabled. The 'Use Case Stakeholder Review' row has a circled number '4' next to it.

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.

The screenshot shows the 'Workflow - Use Case Review' editor. The 'Use Case Stakeholder Review' workflow is displayed with stages: Start, Awaiting Approval, End Approved, and End Rejected. The 'Stage Properties' panel is open on the right, showing the 'Assignees and Subscribers' section. A circled number '6' is next to the section header. A circled number '7' is next to the 'Add Assignee' button.

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)**.

The screenshot shows the 'Workflow - Use Case Review' editor with the 'Use Case Stakeholder Review' workflow. The 'Stage Properties' panel is open, specifically the 'Assignees' section. Step 8 is labeled next to the 'Assign to' dropdown, which has 'A field in a related object' selected. Step 9 is labeled next to the 'Relationship Type' dropdown, which has 'Direct Parent' selected. Step 10 is labeled next to the 'Related Object Type' dropdown, which has 'Use Case' selected. Step 11 is labeled next to the 'Related Object Field' dropdown, which has 'Owner (MRG-ModelUseCaseOwner)' selected.

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

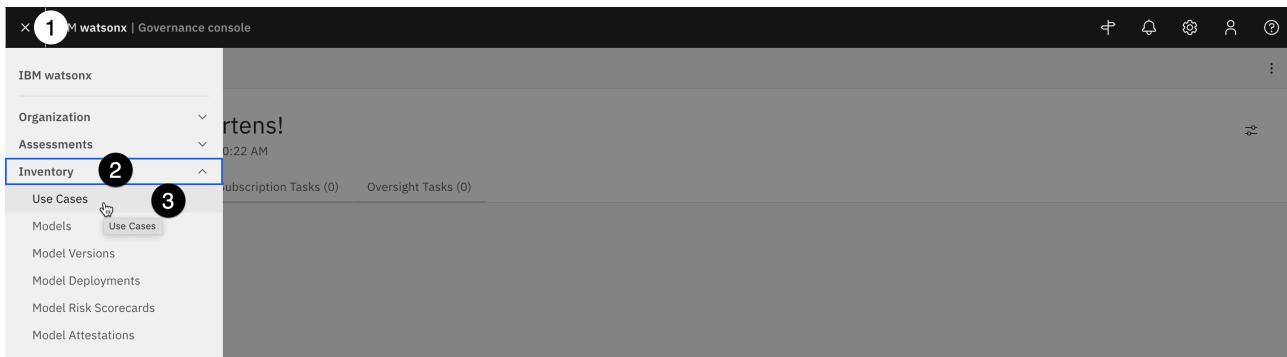
In this section of the lab, you will go through the steps of the approval workflow you customized during the governance console configuration steps. The human resources department has received a large number of applications for open positions, and would like to use AI to summarize them to help save time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

**Use Cases (33)**  
[ View Name : SysView-Grid-Register ]

Name	Purpose	Description	Owner	Status	Risk Level	Tags
<input type="checkbox"/> Agency Based LGD Estimation High Oaks Bank > North America > Corporate Banking		Uses internal and external recovery data, adjusted for macro-economic impact. Uses statistical regression	Bob Eldridge	Approved for Development	Low	
<input type="checkbox"/> Banking book HTM corporate bond - income High Oaks Bank > Europe > Corporate Banking		ALM based income forecast for the HTM portfolio, initially for the CCAR 2013 stress-test. Vendor solution using conditional scenarios and core ALM system.	Bob Eldridge	Approved for Development	Medium	
<input type="checkbox"/> Black model for TD derivatives		Black linear-Nonlinear model on TR process				

4 Active Only **New** +

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**.

**General** ⓘ

* Name *	* Owner *
Resume summarization	admin
Search users	
Purpose	
* Description *	
Summarize resumes from job applicants.	
* Use Case Type	
AI	

**Use Case creation** ⓘ

A **use case** is meant to track and capture information about a collection of models that will be built to serve a particular purpose. A use case should be created whenever there is a business need.

1 item requires attention.

All Key Items (6) ▾

- Name \*
- Owner \*
- Purpose
- Description \*
- Use Case Type

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.

Use Case Details

Uses Foundation Models \* 1

Risk Level

Externally Facing

Proposed Solution

Additional Details

Target Implementation Date

Risk ①

Use Case Data Gathering ①

Please capture all relevant information to this AI use case proposal an then submit using the Action button

Select an action to validate ▾

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.

Risk ①

Risk Level 3

Risk Identification Completion Date

Risk Assessment Completion Date

Risk Identification Assessments

Search

Add New

Name	Description	Progress (%)	Tags
No results			

Stage Use Case Data Gathering (Data gathering) C

Due Date 2/21/2025 ▾

Tags +

No tags have been added yet.

Use Case Data Gathering ①

Please capture all relevant information to this AI use case proposal an then submit using the Action button

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.

Risks

Search

Name	Description	Inherent Risk Rating	Residual Risk Rating	Status	Tags
No results					

Risk Status

Residual Risk Rating

No data available

No data available

Tags +

No tags have been added yet.

Use Case Data Gathering ①

Please capture all relevant information to this AI use case proposal an then submit using the Action button

Select an action to validate ▾

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.

Copy from Library

Task

\* Modified

Name

No r

Risks

No r

Risk Sta

Regu

(MOD\_0000000\_RIS\_0000017)

Library > MRG > AI Risk Library

sensitive features can be inferred about individuals who participated in training a model. These attacks occur when a more

Not Determined Not Determined Not Applicable Input

Confidential data in prompt (MOD\_0000000\_RIS\_0000018)

Library > MRG > AI Risk Library

Inclusion of confidential data as a part of a generative model's prompt, either through the system prompt design or through the inclusion of end user input, might later result in unintended reuse more

Not Determined Not Determined Not Applicable Input Robustness

Evasion attack (MOD\_0000000\_RIS\_0000019)

Library > MRG > AI Risk Library

Evasion attacks attempt to make a model output incorrect results by perturbing the data sent to the trained model. more

Not Determined Not Determined Not Applicable Input Robustness

Extraction Attack (MOD\_0000000\_RIS\_0000020)

Library > MRG > AI Risk Library

An attack that attempts to copy or steal the AI model by appropriately sampling the input space, observing outputs, and building a surrogate model, is known as an extraction attack. more

Not Determined Not Determined Not Applicable Input Robustness

Prompt injection (MOD\_0000000\_RIS\_0000021)

Library > MRG > AI Risk Library

A prompt injection attack forces a model to produce unexpected output due to the structure or information contained in prompts. more

Not Determined Not Determined Not Applicable Input Robustness

Prompt leaking (MOD\_0000000\_RIS\_0000022)

Library > MRG > AI Risk Library

A prompt leak attack attempts to extract a model's system prompt (also known as the system message). more

Not Determined Not Determined Not Applicable Input Robustness

Prompt priming (MOD\_0000000\_RIS\_0000023)

Library > MRG > AI Risk Library

Because generative models tend to produce output like the input provided, the model can be prompted to reveal specific kinds of more

Not Determined Not Determined Not Applicable Input Multi-category

Cancel Done

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 the 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.

The screenshot shows the Watsonx governance platform interface. At the top, there's a navigation bar with 'Use Case' and a dropdown menu. Below it, the title 'Resume summarization' is followed by a star and a downward arrow. The main area has tabs for 'Task', 'Activity', and 'Admin' (which is highlighted). A note at the top left says '\*Modified. Required.\*'. The 'General' section contains the following fields:

- Name:** Resume summarization
- Description:** Summarize resumes from job applicants.
- Owner:** admin
- Use Case Type:** AI
- Status:** Proposed (with a number 11 next to it)
- Risk Level:** (not explicitly shown)

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.

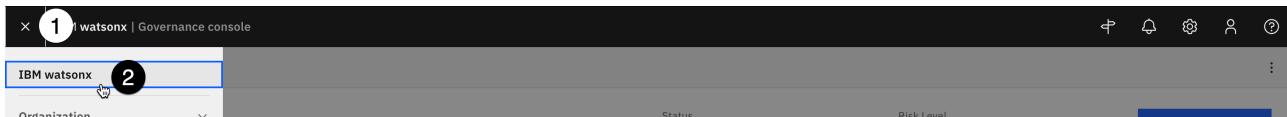
**THESE EVALUATIONS ARE NOT INTENDED TO SHOW THE RELATIVE STRENGTHS OF THE OPENAI OR AZURE PLATFORMS, AND SHOULD NOT BE PRESENTED AS SUCH.** The prompt used in this lab is fairly simple, and in a real-world scenario would be tuned and optimized for the individual use case. The evaluations here are presented 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.

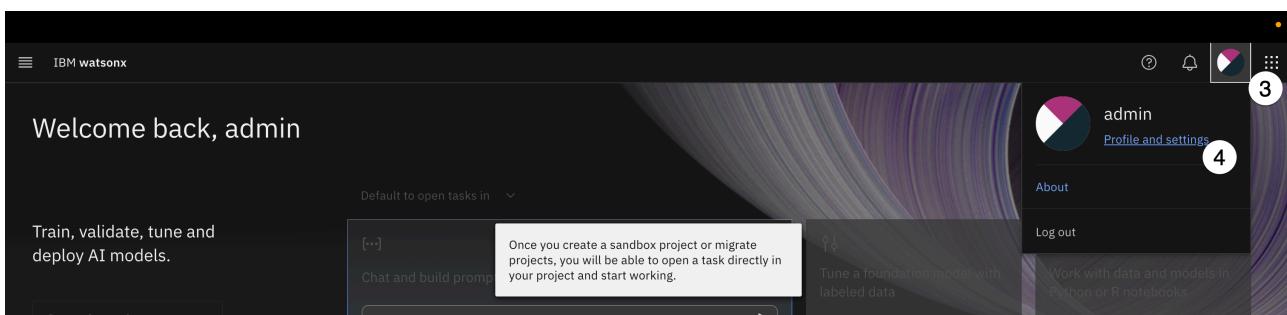
To begin, you will need to gather credentials used by the notebook. From watsonx, you will need the base Cloud Pak for Data URL, as well as the username and password of the created user. You will also create an API key for the user.

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.

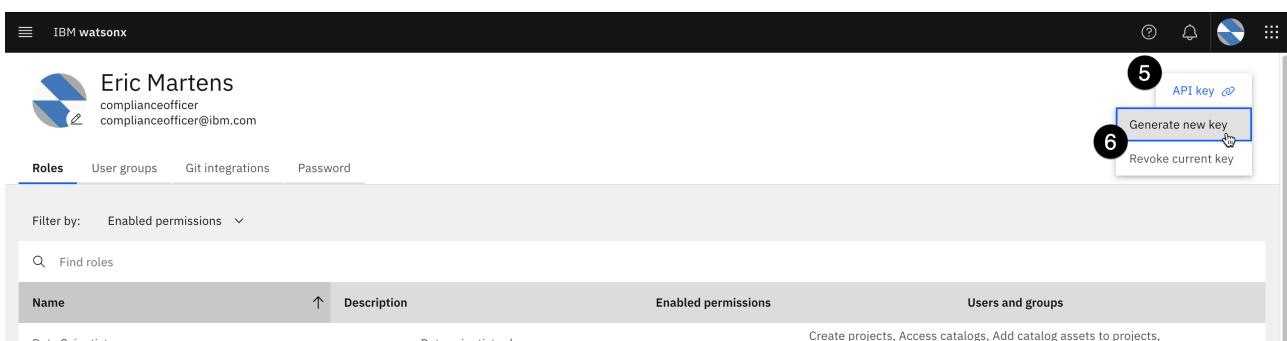
1. From the watsonx governance console, click on the [hamburger menu](#) in the upper left.
2. Click on the [IBM watsonx](#) menu item. The watsonx home page opens in the watsonx context (as opposed to the Cloud Pak for Data context).



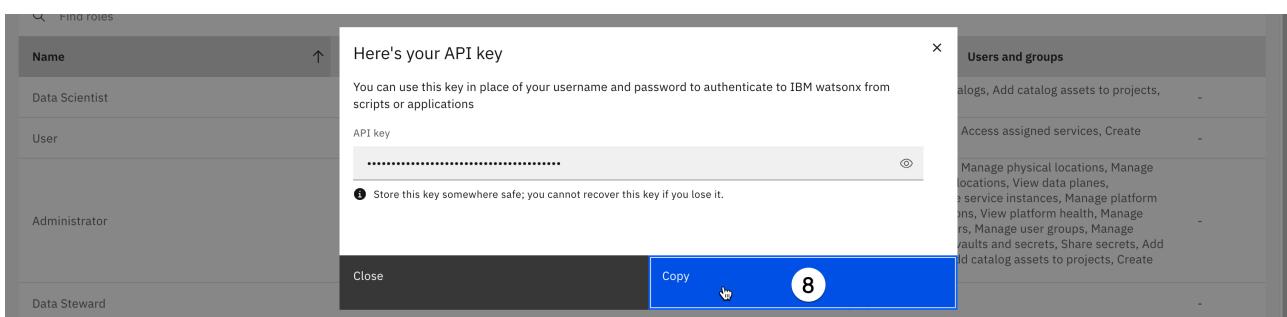
3. Click on the [avatar icon](#) in the upper right to open the user menu.
4. Click on the [Profile and settings](#) item from the menu. The user profile screen opens.



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.



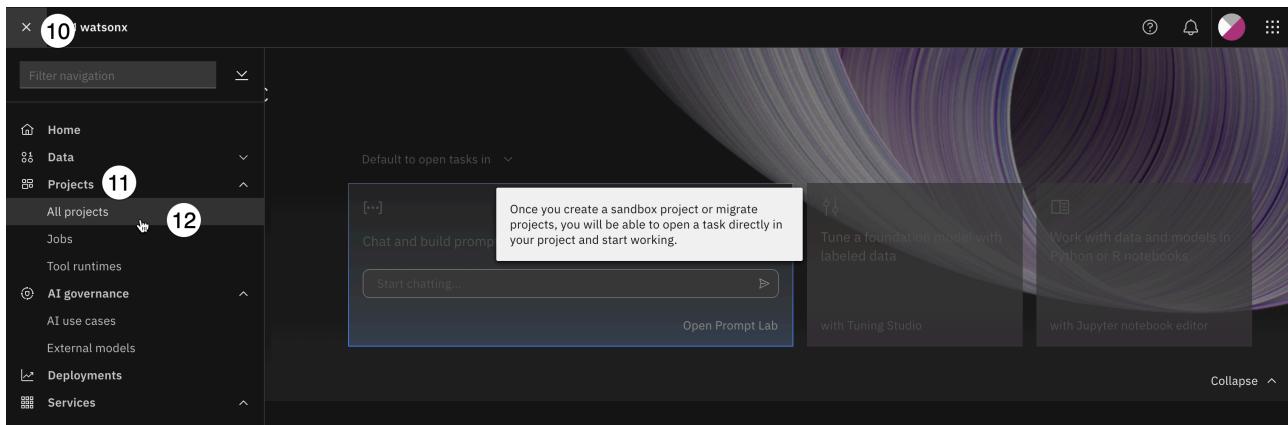
7. Click the red [Generate](#) button to confirm API key creation. Note that, as the warning states, generating a new key will invalidate any existing keys you have.
8. Click the [Copy](#) button to copy your new key to the clipboard. Paste it into a text file for later use in the notebook, where it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

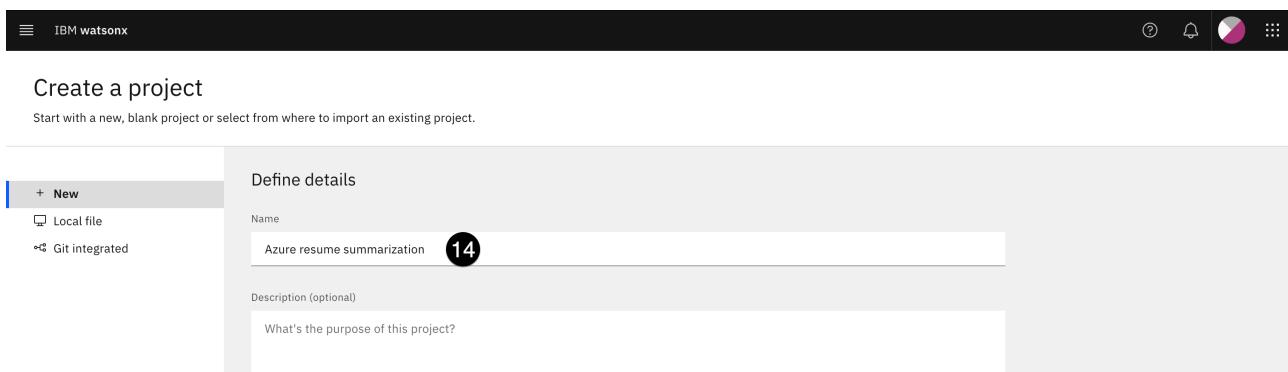
11. Click on the [Projects](#) menu item to expand it.

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.

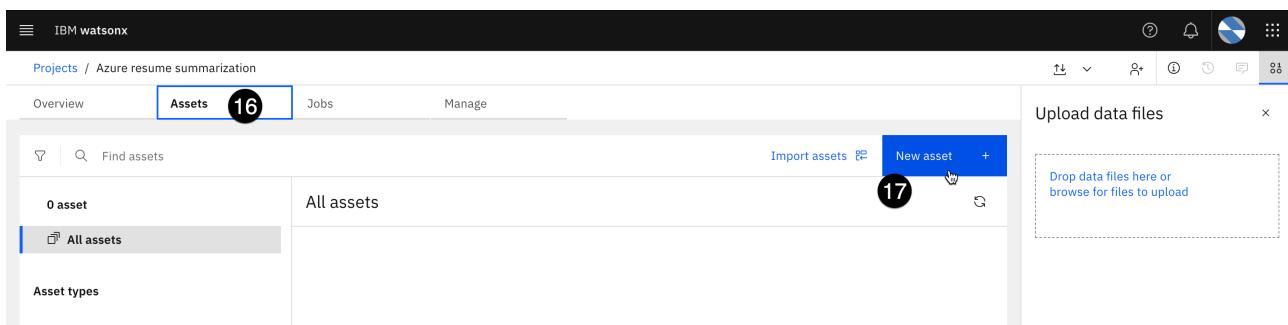
14. Give your project a [Name](#).



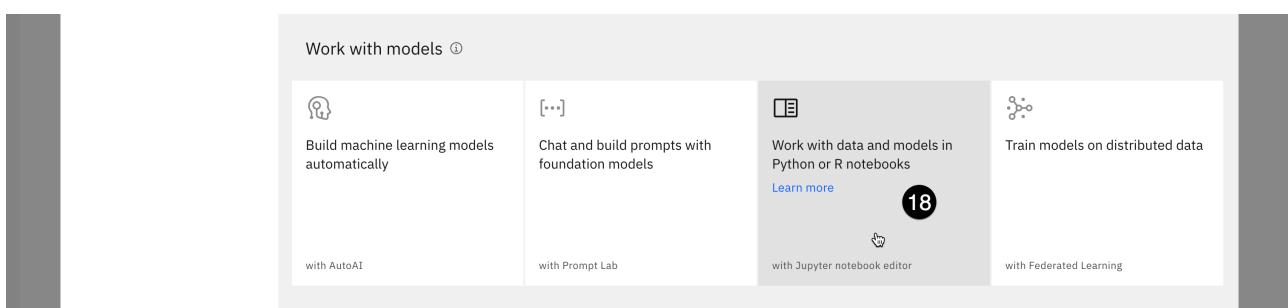
15. Click the [Create](#) button. Your project will be created.

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.

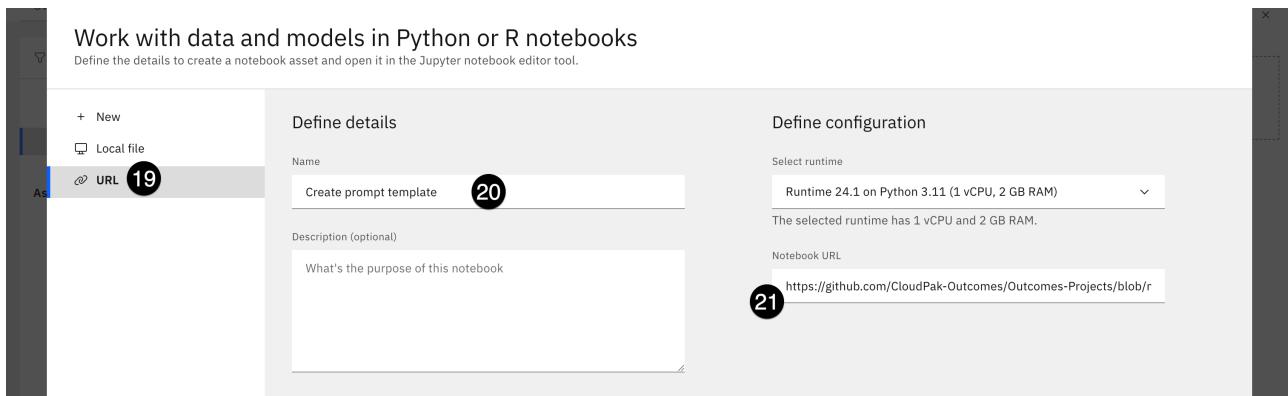


19. Click on the [URL](#) option.

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.

```
[1]: import os
from rich import print
from IPython.display import display, Markdown

CPD_URL = "https://cpd-cpd.apps.67af07431b420a234ba2acca.am1.techzone.ibm.com/"
CPD_USERNAME = "admin"
CPD_API_KEY = "<EDIT THIS>"

AZURE_OPENAI_ENDPOINT = "<EDIT THIS>"
AZURE_OPENAI_DEPLOYMENT_NAME = "<EDIT THIS>"
AZURE_CLIENT_ID = "<EDIT THIS>"
AZURE_CLIENT_SECRET = "<EDIT THIS>"
AZURE_TENANT_ID = "<EDIT THIS>"

PROJECT_ID = os.environ.get('PROJECT_ID', "<YOUR_PROJECT_ID>")
print(f"Your project id is {PROJECT_ID}")
```

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.

This prompt template is not tracked.  
To track a prompt template, add it to an AI use case. Tracking captures details about the asset for governance purposes.  
**Important:** Once you start tracking a prompt template in a use case, you can no longer edit it. Wait until the prompt template is stable to start tracking.

**2**

Learn more

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.

Name	Status	Owner	Inventory	Tags	Risk level	Alerts in
<a href="#">Resume summarization</a> 4	Approved	AD admin	High Oaks Bank Model Inventory		None	None
<a href="#">Finance News Analysis</a>	Approved	AD admin	High Oaks Bank Model Inventory		Low	None
<a href="#">Executive summary generation</a>	Approved	AD admin	High Oaks Bank Model Inventory		Low	None
<a href="#">Customer Attrition</a>	Approved	AD admin	High Oaks Bank Model Inventory		Medium	None

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.

<b>Name</b>	Resume summarization
<b>Description</b>	Summarize resumes from job applicants.
<b>Owner</b>	AD admin
<b>Status</b>	Approved (System, Feb 16, 2025)
<b>Risk level</b>	None
<b>Inventory</b>	High Oaks Bank Model Inventory

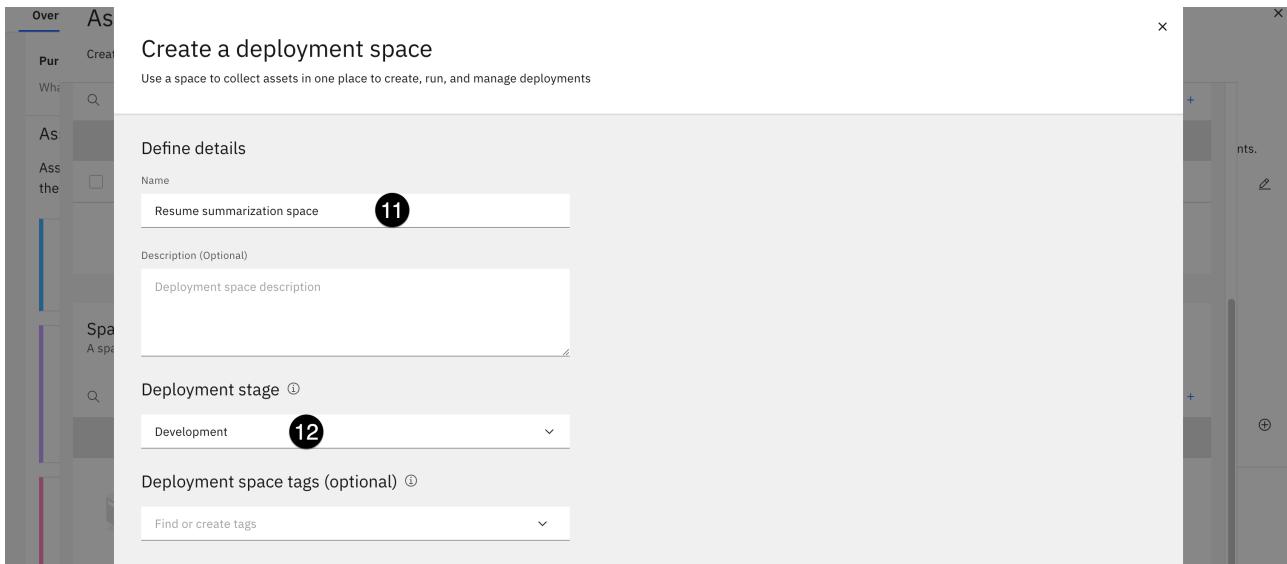
7. Scroll down to the [Projects](#) section of the window and check the box next to the [Azure resume summarization](#) project you created. This associates the project and its assets with the [Development](#) phase of the [Resume summarization](#) use case.
8. Click on the [Save](#) button to save the 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.

- Click on the [Associate workspaces](#) button in the [Validation](#) section. The [Associate workspaces](#) window opens again.

- Scroll down to the [Space](#) section of the window and click on the [New space](#) button. The [Create a deployment space](#) window opens.

- Give your space a [Name](#).
- 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.

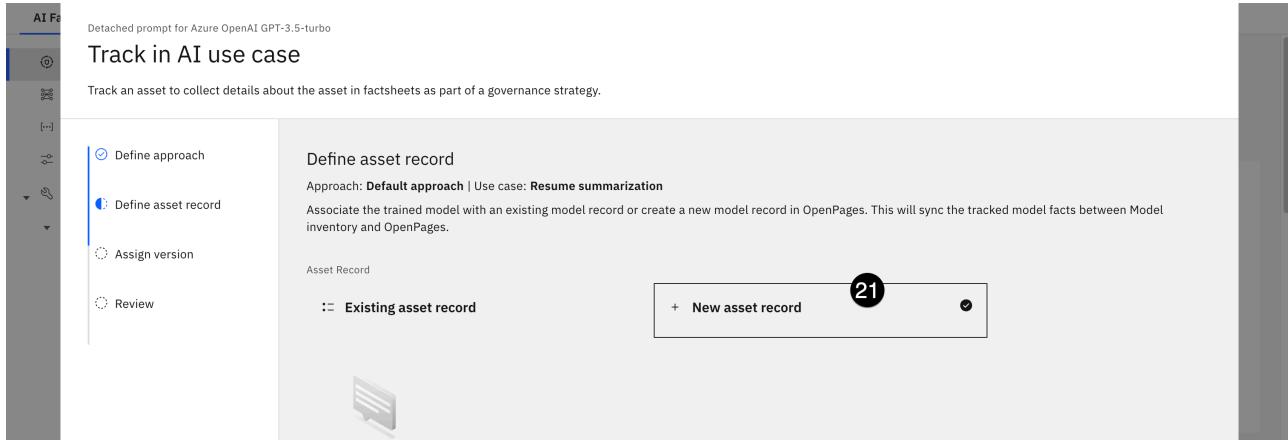
17. Locate the [Detached prompt for Azure...](#) asset from the table, and click on the [three vertical dots](#) to open the context menu.

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.

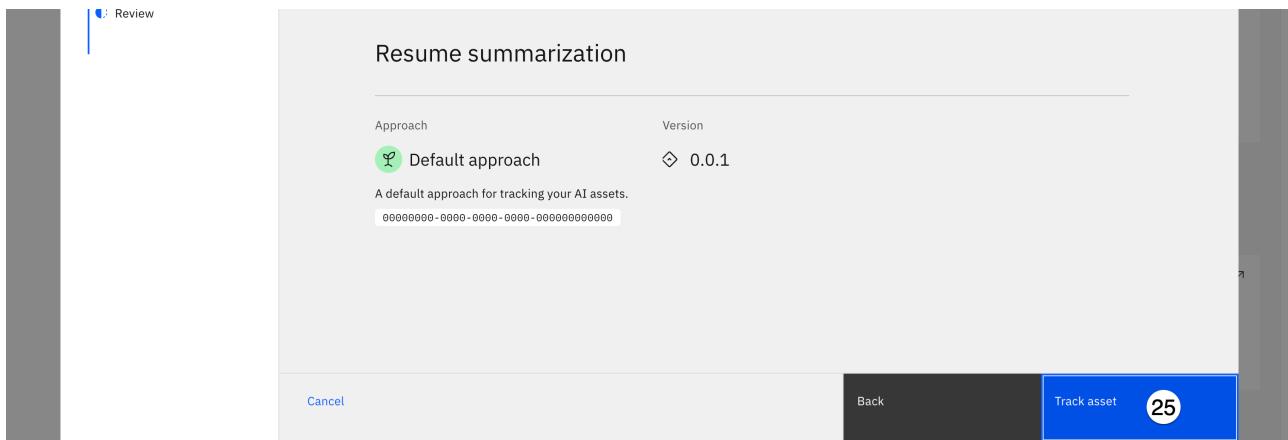


22. Click on the [Next](#) button. The [Assign version](#) screen opens. This screen allows you to set a version number for your model based on its progress in development.

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.

This screenshot shows the IBM WatsonX AI Factsheet interface. At the top, there's a breadcrumb trail: Projects / Azure resume summarization. A notification badge with the number '1' is visible next to the breadcrumb. Below the breadcrumb, there are tabs for 'AI Factsheet' and 'Evaluate'. On the left, a sidebar titled 'Governance' lists 'Foundation model' and 'Prompt template'. The main content area is titled 'Governance' and contains a single item: 'resume summarization\_eval\_data.csv'. On the right side of the main content area, there's a 'Export report' button.

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.

This screenshot shows the 'Assets' tab in the IBM WatsonX interface. The left sidebar shows '3 assets' under 'All assets' and categories for 'Asset types': Data (1), Notebooks (1), and Prompts (1). The main table lists three assets: 'Create prompt template' (Notebook from URL), 'resume\_summarization\_eval\_data.csv' (CSV), and 'Detached prompt for Azure OpenAI GPT-3.5-turbo' (Detached prompt template). The 'resume\_summarization\_eval\_data.csv' row has a context menu open, indicated by a circled '2'. The menu items are 'Promote to space', 'Prepare data', 'Download' (circled '3'), and 'Delete'. To the right of the table, there's an 'Upload data files' section with a dashed box for dropping files.

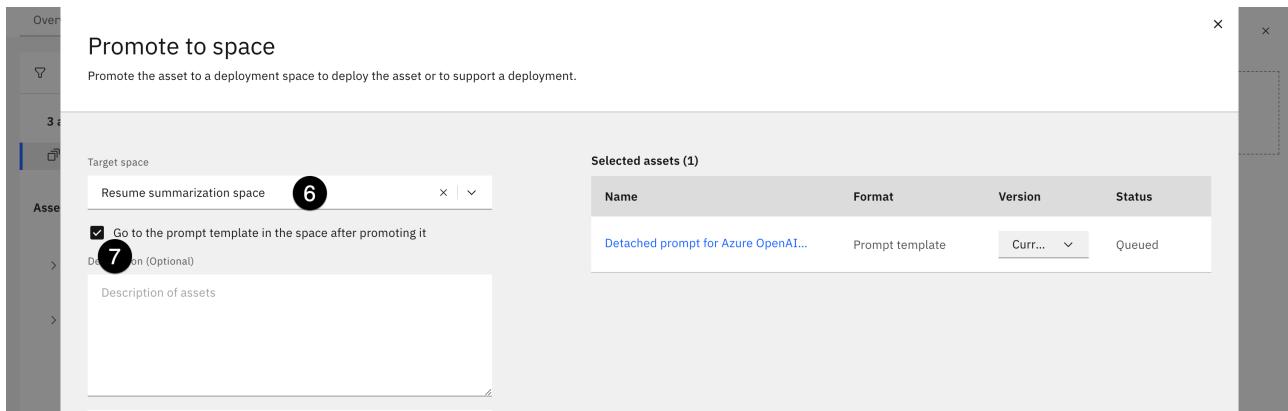
4. From the [Assets](#) tab, click on the [three vertical dots](#) to the right of the [Detached prompt template...](#) to open the context menu.

5. Click on the [Promote to space](#) menu item. The [Promote to space](#) window opens.

This screenshot shows the 'Assets' tab in the IBM WatsonX interface. The left sidebar shows '2 assets' under 'All assets' and categories for 'Asset types': Notebooks (1) and Prompts (1). The main table lists two assets: 'Detached prompt for Azure OpenAI GPT-3.5-turbo' (Detached prompt template) and 'Create prompt template' (Notebook from URL). The 'Create prompt template' row has a context menu open, indicated by a circled '4'. The menu items are 'Evaluate', 'Go to AI factsheet', 'Untrack', 'Promote to space' (circled '5'), and 'Delete'. To the right of the table, there's an 'Upload data files' section with a dashed box for dropping files. A separate 'Promote to space' window is open over the main interface, containing fields for 'Space' (selected 'Evaluation'), 'Name' ('Evaluation'), and 'Description' ('Evaluation').

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.

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

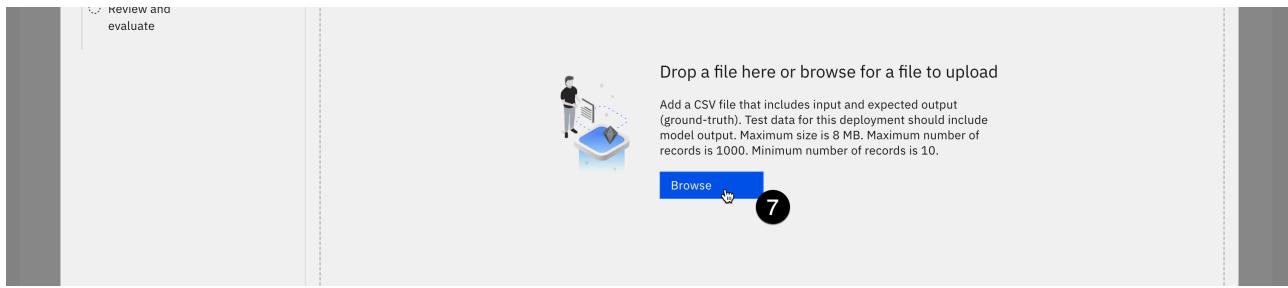
- Click on the Associate a service instance button to associate a machine learning service with the space. The Evaluate a prompt template window opens. By default, the prompt will be evaluated for generative AI quality and model health. However, you can configure the acceptable thresholds for these metrics.

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

- 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.

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

- 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.

Metric	Score	Violation
Rouge	44.54	35.46
SARI		

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

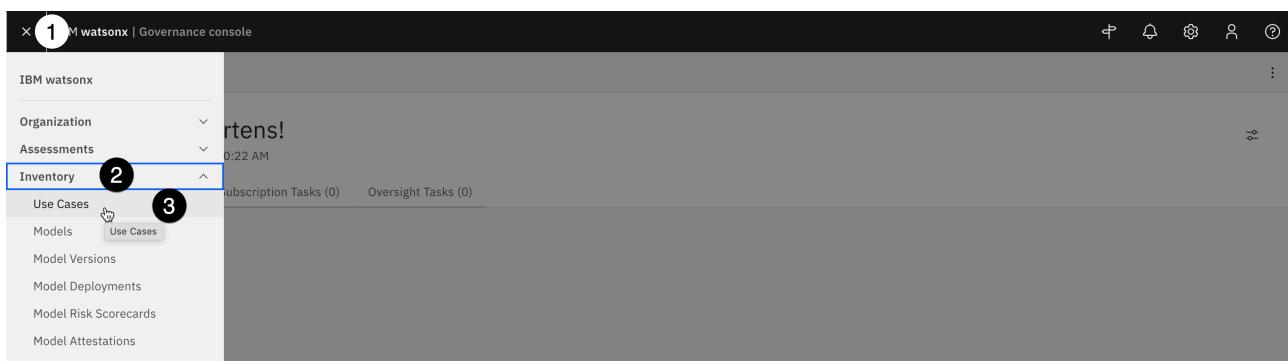
While much of the industry focus has been on ChatGPT and generative AI, the vast majority of models solving real-world business problems in production are traditional predictive machine learning models. Most organizations would significantly benefit from a governance solution for their predictive models,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

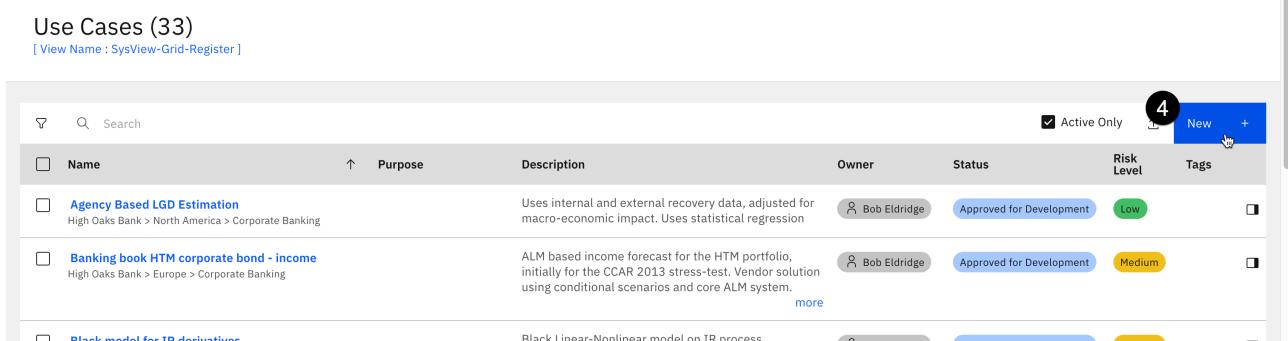


The screenshot shows the IBM Watsonx Governance console interface. At the top, there's a header with a close button, a user icon, and a help icon. Below the header is a dark sidebar with the following menu items:

- IBM Watsonx
- Organization
- Assessments
- Inventory** (highlighted with a blue border and circled with a black number 2)
- Use Cases (highlighted with a blue border and circled with a black number 3)
- Models
- Model Versions
- Model Deployments
- Model Risk Scorecards
- Model Attestations

On the right side of the screen, there's a main content area with a message "It's time to govern!" and two tabs at the bottom: "Subscription Tasks (0)" and "Oversight Tasks (0)".

4. Click the blue [New](#) button. The [New Use Case](#) tab opens.



The screenshot shows the "Use Cases (33)" page. At the top, there's a search bar and a "New" button (circled with a black number 4). Below the search bar is a table with columns: Name, Purpose, Description, Owner, Status, Risk Level, and Tags. There are three entries listed:

Name	Purpose	Description	Owner	Status	Risk Level	Tags
Agency Based LGD Estimation	High Oaks Bank > North America > Corporate Banking	Uses internal and external recovery data, adjusted for macro-economic impact. Uses statistical regression	Bob Eldridge	Approved for Development	Low	
Banking book HTM corporate bond - income	High Oaks Bank > Europe > Corporate Banking	ALM based income forecast for the HTM portfolio, initially for the CCAR 2013 stress-test. Vendor solution using conditional scenarios and core ALM system.	Bob Eldridge	Approved for Development	Medium	
Black model for TD derivatives		Black Linear-Nonlinear model on TR process				

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**.

The screenshot shows the 'General' tab of the 'Use Case creation' form. The 'Name' field (5) contains 'Application screening'. The 'Owner' field (6) shows 'admin' with a search icon. The 'Description' field (7) contains 'Screen applicants for positions'. The 'Use Case Type' dropdown (8) has 'AI' selected. A sidebar on the right lists validation rules: '1 item requires attention.' and 'All Key Items (6)'. The validation items are: Name\*, Owner\*, Purpose, Description\*, and Use Case Type.

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.

The screenshot shows the 'Business Entities' section of the form. The 'Primary Business Entity' tab is selected. An 'Add' button (9) is highlighted with a mouse cursor. A sidebar on the right lists filter options: Name\*, Owner\*, Purpose, Description\*, Use Case Type, and Primary Business Entity\*.

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.

The screenshot shows the 'Add' window with the 'Business Entities' list. The 'Human Resources' entity (10) is selected and highlighted with a checkmark. The 'Done' button (11) at the bottom is highlighted with a mouse cursor.

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.

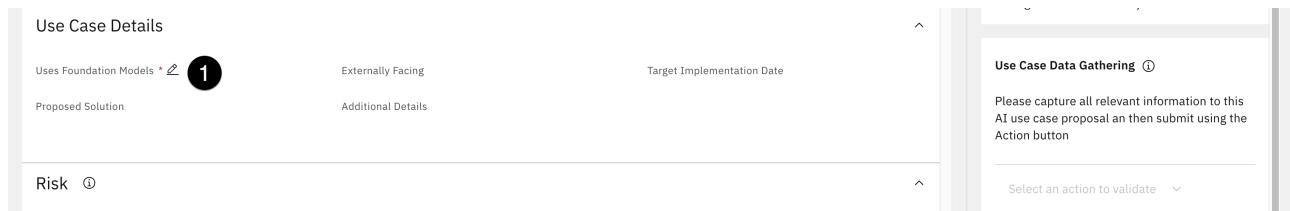
## 2. Progress the predictive model use case to the next phase

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.

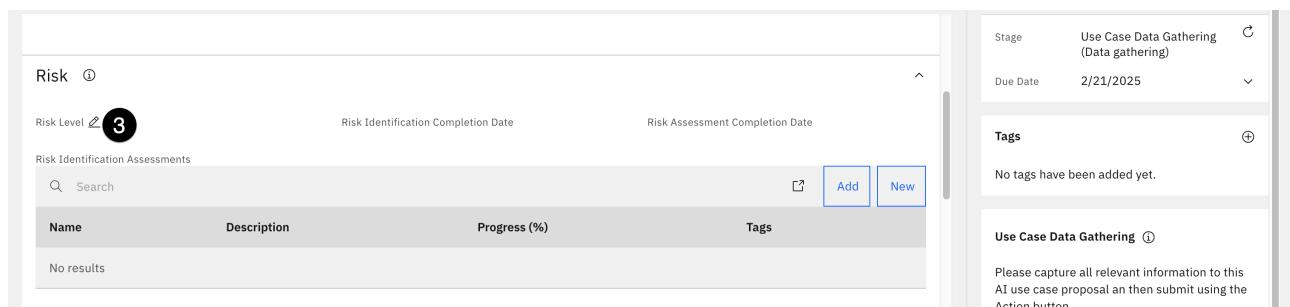


The screenshot shows the 'Use Case Details' section of a form. On the left, there is a table with columns for 'Proposed Solution', 'Externally Facing', and 'Additional Details'. Below this is a section titled 'Risk' with a help icon. On the right, there is a large panel titled 'Use Case Data Gathering' with a help icon. It contains instructions: 'Please capture all relevant information to this AI use case proposal and then submit using the Action button'. At the bottom of this panel is a dropdown menu labeled 'Select an action to validate'.

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.



The screenshot shows the 'Risk' section of a form. On the left, there is a table with columns for 'Name', 'Description', 'Progress (%)', and 'Tags'. A search bar and 'Add' and 'New' buttons are also present. On the right, there is a panel titled 'Use Case Data Gathering (Data gathering)' with a help icon. It shows a 'Stage' of 'Use Case Data Gathering (Data gathering)', a 'Due Date' of '2/21/2025', and a 'Tags' section stating 'No tags have been added yet.' Below this is another panel titled 'Use Case Data Gathering' with a help icon, containing the same instructions as the first panel.

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.

Risks

Search

Name	Description	Inherent Risk Rating	Residual Risk Rating	Status	Tags
No results					

Risk Status

No data available

Residual Risk Rating

No data available

Tags

No tags have been added yet.

Use Case Data Gathering ⓘ

Please capture all relevant information to this AI use case proposal an then submit using the Action button

Select an action to validate ▾

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.

Copy from Library

(MOD\_0000000\_RIS\_0000017) Library > MRG > AI Risk Library

sensitive features can be inferred about individuals who participated in training a model. These attacks occur when an

**Confidential data in prompt** (MOD\_0000000\_RIS\_0000018) Library > MRG > AI Risk Library

Inclusion of confidential data as a part of a generative model's prompt, either through the system prompt design or through the inclusion of end user input, might later result in unintended reuse

**Evasion attack** (MOD\_0000000\_RIS\_0000019) Library > MRG > AI Risk Library

Evasion attacks attempt to make a model output incorrect results by perturbing the data sent to the trained model.

**Extraction Attack** (MOD\_0000000\_RIS\_0000020) Library > MRG > AI Risk Library

An attack that attempts to copy or steal the AI model by appropriately sampling the input space, observing outputs, and building a surrogate model, is known as an extraction attack.

**Prompt injection** (MOD\_0000000\_RIS\_0000021) Library > MRG > AI Risk Library

A prompt injection attack forces a model to produce unexpected output due to the structure or information contained in prompts.

**Prompt leaking** (MOD\_0000000\_RIS\_0000022) Library > MRG > AI Risk Library

A prompt leak attack attempts to extract a model's system prompt (also known as the system message).

**Prompt priming** (MOD\_0000000\_RIS\_0000023) Library > MRG > AI Risk Library

Because generative models tend to produce output like the input provided, the model can be prompted to reveal specific kinds of

Cancel Done

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 the 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.

Use Case

Application screening ⋆ ^

Task Activity Admin **10**

\*Modified Required\*

General ⓘ

Name \* Application screening

Owner admin

Use Case Type AI

Purpose

Description Screen applicants for positions

Status ⓘ **11** Proposed

Risk Level High

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.

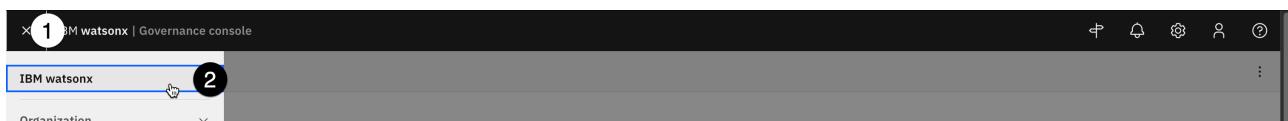
In the next steps of the lab, you will connect watsonx.governance to this model and configure it for evaluations.

### 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.

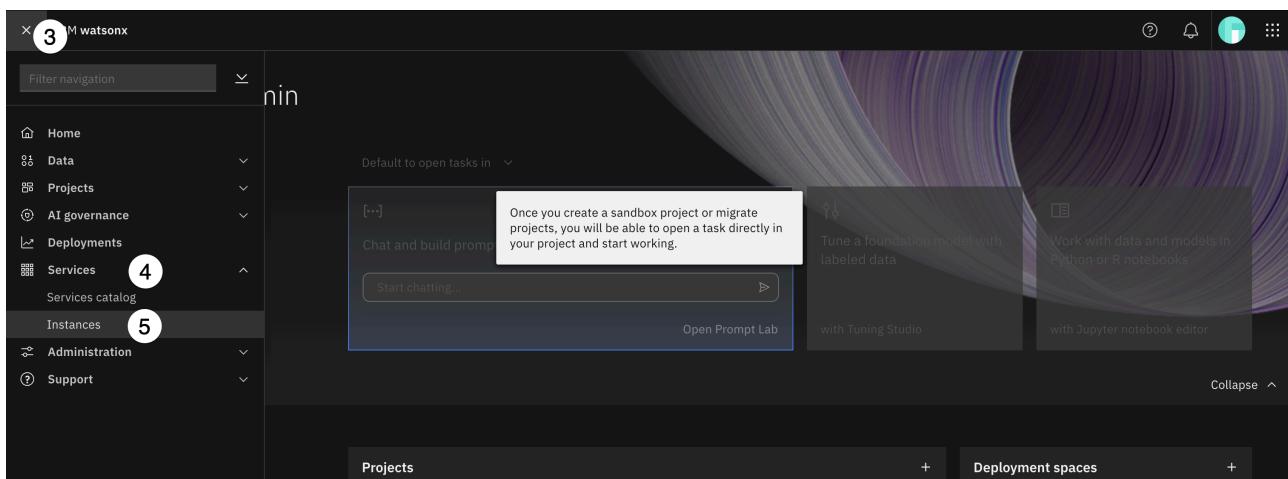
2. Click on the **IBM watsonx** menu item. The watsonx home screen opens.



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.

## Instances

Last updated: 10/29/2024 10:28 PM ⓘ

Filter by: Type ▾ Status ▾ Data plane ▾ Physical location ▾								
Name	Type	Created by	vCPU requests	Memory requests (GiB)	Data plane	Physical location	Status	Created on
cpd-database Service instance for db2oltp-17...	db2oltp	admin	2.10	4.25 Gi	—	—	Green	Oct 29, 2024
openscale-defaultinstance IBM Watson OpenScale	aios	admin	0.00	0.00 Gi	—	—	Green	Oct 29, 2024
openpagesinstance-cr OpenPages Instance	openpages	admin	4.45	12.40 Gi	—	—	Green	Oct 29, 2024

## 4. Add the SageMaker model to the dashboard

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

IBM Watsonx

Need help? ⓘ

Insights dashboard

Refresh ⓘ Add to dashboard +

Deployments	Quality Alerts	Fairness Alerts	Drift v2 Alerts	Drift Alerts	Global explanation Alerts	Custom Alerts
1	3	1	3	--	--	--

Filter by Tags ▾ Alert type ▾ Machine learning provider ▾ Sort by Severity ▾

Q Which deployment are you looking for?

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

- Click on the **Add machine learning provider** button.

IBM Watsonx

Need help? ⓘ

System setup

Connect to a database, machine learning providers, and integrated services. Optionally enable batch support.

Required

- Database
- Machine learning providers
- Users & roles

Optional

- Metric groups
- Metric endpoints
- Batch support
- Integrations

Machine learning providers

Description

Watson OpenScale connects to deployed models stored in a machine learning environment.

Add machine learning provider +

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

System setup

Connect to a database, machine learning providers, and integrated services. Optionally enable batch support.

**Required**

- Database
- Machine learning providers** (selected)
- Users & roles

**Optional**

- Metric groups
- Metric endpoints
- Batch support
- Integrations

**Machine learning providers**

**New provider**

Description

Click edit to enter provider description.

**Connection**

Click edit to enter the connection information.

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.

System setup

Connect to a database, machine learning providers, and integrated services. Optionally enable batch support.

**Required**

- Database
- Machine learning providers** (selected)
- Users & roles

**Optional**

- Metric groups
- Metric endpoints
- Batch support
- Integrations

**Machine learning providers**

**Connection**

**SageMaker development**

Description

Connect to the provider where your deployed models are stored and specify if the environment is a pre-production or production environment.

**Pre-production environments**

Test models by uploading test data sets (csv files) and running evaluations. When the model is ready, approve it for production.

**Production environments**

Monitor production models by logging model transactions and sending feedback (labeled test data) to Watson OpenScale for continuous evaluation.

**Service provider**

Choose an option

- Watson Machine Learning (V2)
- IBM SPSS Collaboration & Deployment Services
- Custom Environment
- Amazon SageMaker** (selected)
- Microsoft Azure ML Studio
- Microsoft Azure ML Service

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.

**Machine learning providers** (selected)

**SageMaker development**

Description

Connect to the provider where your deployed models are stored and specify if the environment is a pre-production or production environment.

**Pre-production environments**

Test models by uploading test data sets (csv files) and running evaluations. When the model is ready, approve it for production.

**Production environments**

Monitor production models by logging model transactions and sending feedback (labeled test data) to Watson OpenScale for continuous evaluation.

Note that batch deployments require a custom service provider.

**Access key ID**

AKIA4MTWG6TWGVFZGWJ (8)

**Credential values**

Enter manually

**Secret access key**

..... (9)

**Region**

us-west-1 (10)

**Environment type**

Pre-production  Production

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.

The screenshot shows the 'System setup' page under the 'Required' section. The 'Machine learning providers' checkbox is selected. On the right, there's a list of providers: 'SageMaker development' (Amazon SageMaker), 'service-provider-space-f...' (Watson Machine Learning), and another 'service-provider-space-f...' entry. A blue button at the top right says 'Add machine learning provider'.

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.

The screenshot shows the 'Select a model deployment' window. Under 'Select model location', the 'Machine learning Providers' button is highlighted with a blue circle containing the number 14. Below it is a table listing three providers:

Name	Machine learning Provider	Space name	Environment type
SageMaker development	Amazon SageMaker	-	Pre-production
service-provider-space-fbd60854-e251-4d63-b72d-64813e985452	Watson Machine Learning	application screening development	Pre-production
service-provider-space-fbd60854-e251-4d63-b72d-64813e985452	Watson Machine Learning	application screening development	Pre-production

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.

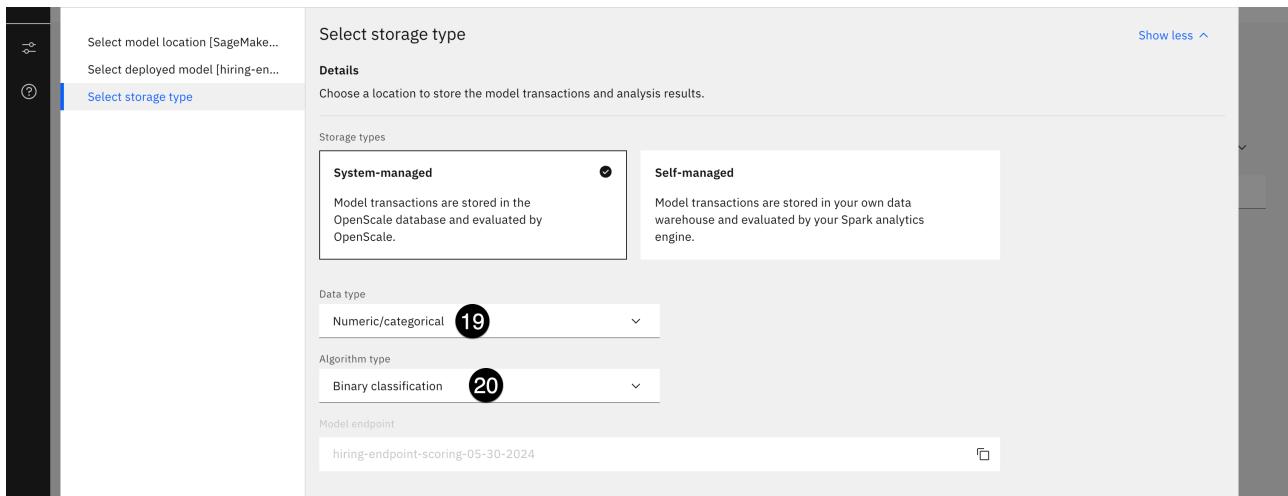
The screenshot shows the 'Select a deployed model' window. The 'Select deployed model' button is highlighted with a blue circle containing the number 17. Below it is a table listing two deployments:

Deployment	Description	Created	Added
credit-risk-endpoint-scoring-05-30-2024		Thu, May 30, 2024, 11:56 AM MDT	
hiring-endpoint-scoring-05-30-2024		Thu, May 30, 2024, 11:54 AM MDT	

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 [hirings\\_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.

Select the feature columns			
	Type	Categorical	Label / Target
<input checked="" type="checkbox"/> Features (19)			
<input type="checkbox"/> HIRED	♂		<input checked="" type="checkbox"/> 5
<input checked="" type="checkbox"/> Age	♂	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> BusinessTravel	♂	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Education	♂	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> RelevantEducationLevel	♂	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> JobLevel	♂	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> MaritalStatus	♂	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> NumCompaniesWorked	♂	<input type="checkbox"/>	<input type="checkbox"/>

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.

The screenshot shows a table of features with their types and categories. The 'IsFemale' feature is highlighted with a red border and a circled number '7' next to it. The table includes columns for feature name, type, category, and checkboxes for selection.

Feature	Type	Category	Action
YearsAtCurrentCompany	8:1		<input type="checkbox"/>
RelevantExperience	8:1		<input type="checkbox"/>
JobType	8:1		<input type="checkbox"/>
SalaryExpectation	8:1		<input type="checkbox"/>
IsFemale	8:1	Categorical	<input checked="" type="checkbox"/> 7

Items per page: 25 | 1 - 19 of 19 items | Back | Next | 8

9. Check the **Prediction** box for the **predicted\_label** field.

10. Check the **Probability** box for the **score** field.

The screenshot shows the 'Select model output' configuration screen. The 'Details' section describes selecting prediction and probability columns. The 'predicted\_label' column is highlighted with a red border and a circled number '9'. The 'score' column has its 'Probability' checkbox checked and a circled number '10' next to it.

Select configuration method  
Specify training data  
Select features and label  
**Select model output**

Select model output

**Details**  
From the model output data, select the column that contains the prediction generated by the deployed model. Select the prediction probability column which contains the model's confidence in the prediction.

Select the prediction and probability column(s)

Features (2)	Type	Prediction	Probability
score	8:1	<input type="checkbox"/>	<input checked="" type="checkbox"/> 10
predicted_label	8:1	<input checked="" type="checkbox"/> 9	<input type="checkbox"/>

Show less ^

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**.

The screenshot shows the 'application screening - dev' configuration interface. The 'Explainability' section is expanded, showing 'General settings' selected (circled with '1'). The 'Model details' and 'Configuration package' sections are also visible.

application screening - dev

**Model info**

- Model details** (selected)
- Endpoints
- Explainability**
  - General settings** (selected) (circled with '1')
  - SHAP
  - LIME (enhanced)
- Evaluations
- Fairness
- Quality

**Model details**

Description: Provide information about the training data and deployed model output to prepare Watsonx for monitoring and providing explanations for model transactions.  
Reconfigure model

**Configuration package**

Package file (File name is not available)

**Training data label**

Label column: HIRED

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).

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

Values	Favorable	Unfavorable
0	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.

The screenshot shows the 'Select the fields to monitor' interface. On the left, a sidebar lists 'Model info', 'Endpoints', 'Explainability' (selected), 'General settings', 'SHAP', 'LIME (enhanced)', and 'Evaluations' (selected). Under 'Evaluations', 'Fairness' is selected. In the center, a callout box highlights 'Recommended features' for Age, TotalWorkingYears, and YearsAtCurrentCompany. On the right, a table titled 'Select one or more fields' shows a list of fields: Age, TotalWorkingYears, YearsAtCurrentCompany, BusinessTravel, Education, InterviewScore, IsFemale, JobLevel, and JobType. The 'IsFemale' row has a checked checkbox in the 'Fields' column, circled with a black circle labeled '15'. Other rows have unchecked checkboxes. A red box highlights the 'Fields' column header. A red box also highlights the 'Age', 'TotalWorkingYears', and 'YearsAtCurrentCompany' rows.

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.

The screenshot shows the 'Specify the monitored groups for [IsFemale]' interface. On the left, a sidebar lists 'Model info', 'Endpoints', 'Explainability' (selected), 'General settings', 'SHAP', 'LIME (enhanced)', and 'Evaluations' (selected). Under 'Evaluations', 'Fairness' is selected. In the center, a callout box highlights the 'Values' column of a table on the right where '0-0' is checked 'Monitored' and '1-1' is checked 'Reference'. A red box highlights the 'Values' column header. A red box also highlights the 'Monitored' and 'Reference' columns of the table.

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.

The screenshot shows the Watson OpenScale interface for 'application screening - dev'. On the left, a sidebar lists various monitors: Model info, Explainability, Evaluations, and Drift v2. The 'Evaluations' section is expanded, showing Quality, Drift v2, Drift, Generative AI Quality, and Model health. The 'Quality' item is selected and highlighted with a blue border and a circled number '1'. In the main panel, the 'Quality' monitor is detailed. It has a 'Description' section stating: 'The Quality monitor evaluates how well your model predicts accurate outcomes. It identifies when model quality declines, so you can retrain your model appropriately.' Below this is a note: 'Note: The Quality metric measures the model's ability to correctly predict outcomes that match labeled data (ground truth) provided by humans. The quality metrics evaluated are standard data science statistics based on model type. [Learn more.](#)' To the right, there is a 'Quality thresholds' section with an 'Edit' button (circled '2').

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.

The screenshot shows the Watson OpenScale interface for 'application screening - dev'. The left sidebar shows the same monitor list as the previous screenshot, with 'Drift v2' selected and highlighted with a blue border and a circled number '6'. The main panel displays the 'Drift v2' monitor details. It includes a 'Description' section: 'The Drift monitor checks if your deployments are up-to-date and behaving consistently. Model input/output data is analyzed in relation to the training/baseline data.' To the right, there are two sections: 'Compute the drift archive' (with an 'Edit' button circled '7') and 'Drift thresholds' (with an 'Edit' button). Below these is a 'Important features' section with an 'Edit' button.

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.

model. For example, a small amount of drift in an important feature may have a bigger impact on the model than a moderate amount of drift in a less important feature.

Note: When SHAP is configured, the important features are automatically detected using the model's global explanation. As SHAP is not configured, you must indicate the important features manually.

**Select from list**

Select up to 100 important features.

**Upload list**

Generate a global explanation and upload the list of important features as a json file. Some snippets/examples to extract this information for popular ML frameworks has been provided on this [wiki](#).

**Features (18)**

	Type
<input type="checkbox"/> Age	81
<input type="checkbox"/> BusinessTravel	88
<input type="checkbox"/> Education	81
<input checked="" type="checkbox"/> InterviewScore	88
<input type="checkbox"/> IsFemale	81
<input type="checkbox"/> JobLevel	88
<input type="checkbox"/> JobType	81
<input type="checkbox"/> MaritalStatus	88
<input type="checkbox"/> NumCompaniesWorked	81

**10** **11**

Back Next

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.

**16**

**Drift v2**

Description

The Drift monitor checks if your deployments are up-to-date and behaving consistently. Model input/output data is analyzed in relation to the training/baseline data.

Compute the drift archive

Status

Training complete

**Model info**

Model details

Endpoints

Explainability

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

**17**

SageMaker development hiring-endpoint-scoring-05-3...

Issues

- Quality
- Fairness
- Drift v2
- Drift
- Global explanation
- Custom

Evaluation pending

SPACE\_Resume summarization space

OpenAI Resume Summarization

Issues

- Quality
- Fairness
- Drift v2
- Drift
- Global explanation
- Custom

Evaluation pending

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.

The screenshot shows the IBM Cloud Pak for Data interface with the 'application screening - dev' workspace selected. The 'Evaluations' tab is active. A context menu is open over the 'Evaluate now' button in the 'Actions' section, with the 'Evaluate now' option highlighted. Other options in the menu include 'Configure monitors' and 'View model information'.

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.

The screenshot shows the 'Import test data' panel. The 'Import' dropdown is set to 'from CSV file'. The 'Test data set' field contains the path 'hiring\_evaluation\_data.csv'. The 'Evaluate' button is visible at the top of the panel.

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.

The screenshot shows the IBM Cloud Pak for Data interface. The top navigation bar includes a search bar and icons for notifications and user profile. The left sidebar contains links for Home, Data, Projects, Catalogs, AI governance (with a badge '3'), External models (with a badge '4'), Deployments, Services, and Instances. The main content area features sections for 'age users' and 'Stay informed'. Below these are three cards: 'Alerts' (No alerts to display), 'Recent projects' (factsheet experiments, Today at 10:32 PM; hiring model development, Yesterday at 11:33 PM), and 'Requests' (No data available). A context menu is open over a hiring model entry, with items like 'Track in AI use case...', 'Delete', and '...'.

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.

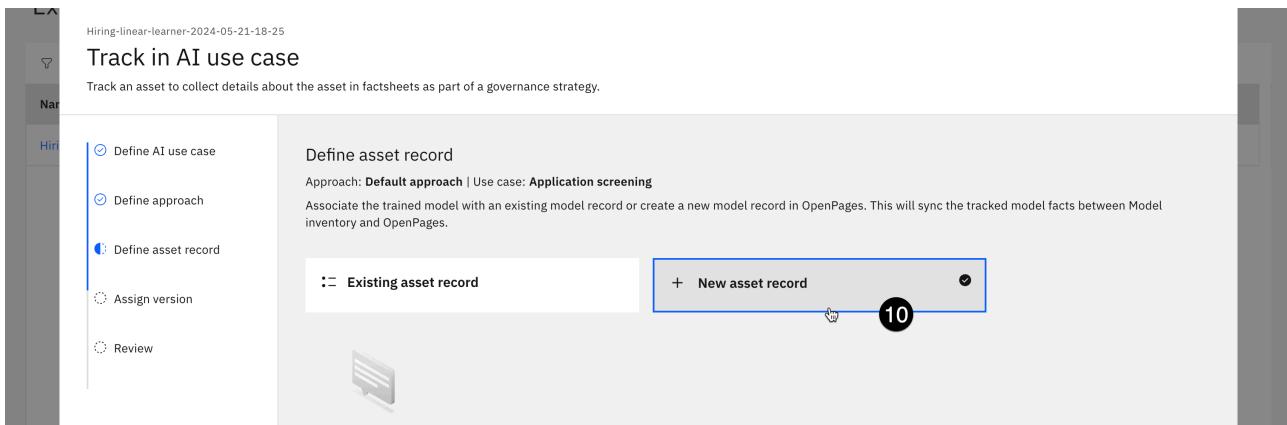
The screenshot shows the 'External models' screen. The top navigation bar and sidebar are similar to the previous screenshot. The main content area displays a table of external models. One row is selected, showing details: Name (Hiring-linear-learner-2024-05-21-18-25), Provider (..), Owner (AD admin), Inventory (Platform assets catalog), AI use case (n/a), and Phase (Validate). A context menu is open over this row, with a '6' badge above the 'Track in AI use case...' option.

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.

The screenshot shows the 'Track in AI use case' window. The top navigation bar and sidebar are present. The main content area is titled 'Define AI use case' and includes a search bar for 'Find AI use cases'. A table lists AI use cases with columns: Name, Status, Owner, Inventory, and Risk level. The 'Application screening' use case is selected, indicated by a '7' badge. Other entries include 'Resume summarizations' (Under Development) and 'Resume summarization' (Rejected).

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.

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



- 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.
- Click on the **Next** button. The **Review** window opens.
- Click on the **Track asset** button to begin 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.

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

Name	Provider	Owner	Inventory	AI use case	Phase	⋮
Hiring-linear-learner-2024-05-21-18-25	--	admin	High Oaks Bank Model Inventory	Application screening	Validate	1

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.

- 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.