Introduction

Identifying potential risks inherent in a use case is a critical part of any AI governance strategy.

These instructions were written for OpenPages 9.1.0.1, running on Cloud Pak for Data 5.2.0 as provisioned in TechZone. Note that subsequent versions of the watsonx governance console (OpenPages), Cloud Pak for Data, and IBM Software Hub may alter the terminology and screens involved with the product. Please contact the lab authors with any major discrepancies. Every effort will be made to keep the lab updated.

This lab assumes that you have performed the actions specified in the **watsonx.governance Level 4 for Practitioners - environment configuration** lab, and are logged into that environment.

Use case

For this lab, you will be performing a post-purchase engagement with GlobalCorp, which has purchased the watsonx.governance solution. You will need to work with them to understand relevant risks in their industry, and applicable controls. You will then create a custom questionnaire for stakeholders to fill out to help identify those risks.

Additional labs in the watsonx.governance Level 4 for Practitioners will explore user management and workflows.

Add to the risk library

The watsonx.governance solution comes with an extensive library of risks associated with AI, drawn from the open-source AI risk atlas. These are maintained in the governance console library, and can be edited or deleted as necessary. For this lab, you will add a new risk to the existing atlas.

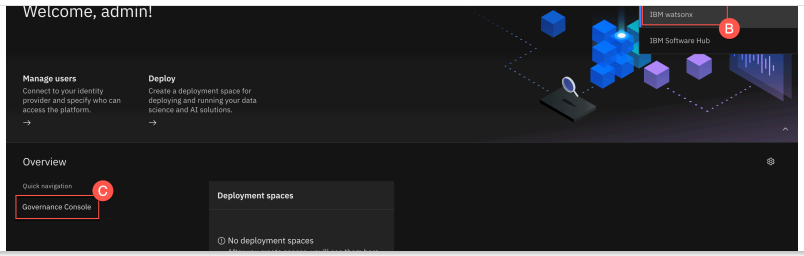
GlobalCorp is interested in cutting-edge agentic AI technologies, which are associated with risks in addition to those present when using standalone generative prompts. A good summary of some of these risks and potential mitigations can be found in a whitepaper from the OWASP GenAI Security Project.

In this lab, you will create a risk associated with *Identity Spoofing & Impersonation*, which is when attackers exploit authentication mechanisms to impersonate AI agents, enabling them to execute unauthorized actions under false identities.

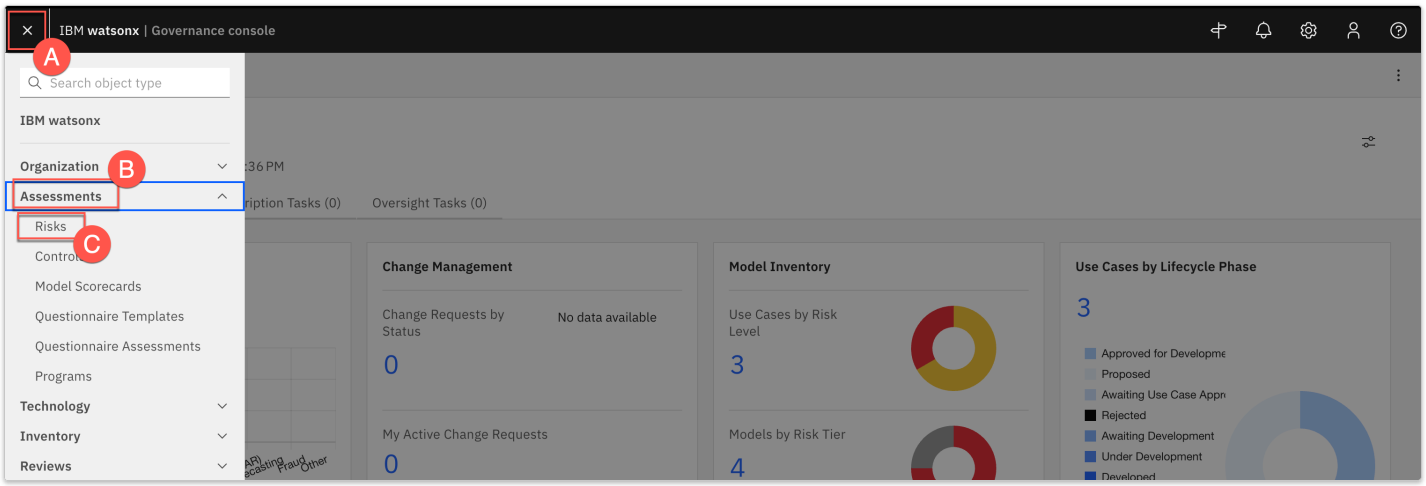
1. Explore the risk library

First, you will locate the governance console risk library and briefly explore the existing risks.

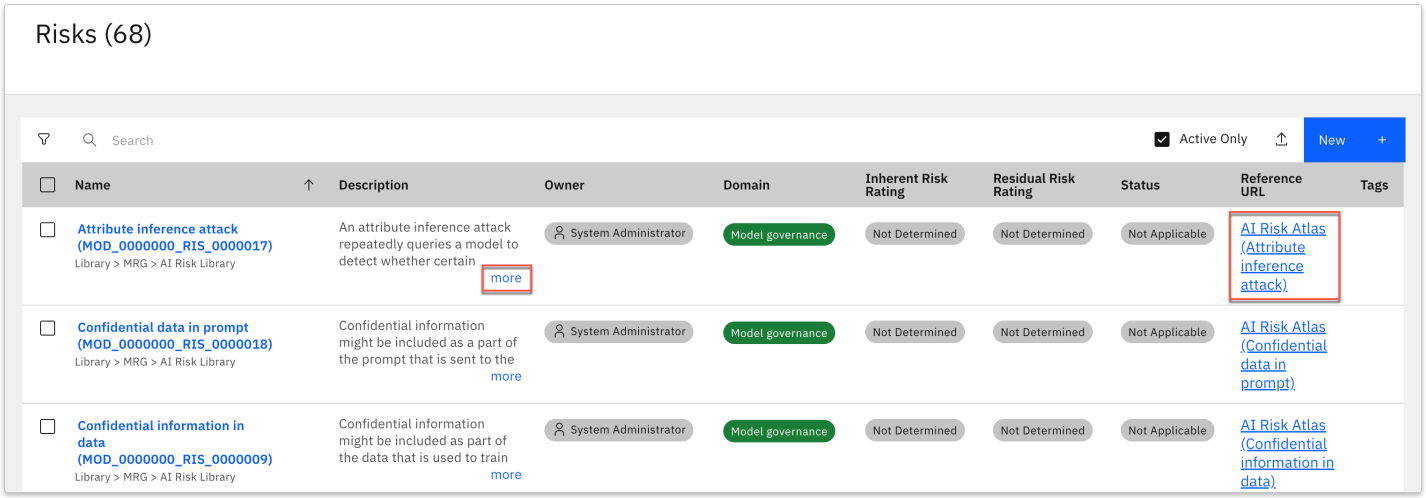
1. Sign into your watsonx environment, and click on the **Change locations** button at the top right (A). Click on the **IBM watsonx** location (B) to switch to it. Click on the **Governance Console** link (C) from the **Quick navigation** section. If the governance console link is not present, you may need to launch it from the list of instances.



2. Click on the **primary menu** icon (A) in the top left to open the menu. Click on the **Assessments** menu item (B) to expand it. Click on the **Risks** menu item (C). The **Risks** tab opens in your workspace.



3. Take a moment to review some of the risks. Note that you can click on the **more** link in the **Description** field for a brief description of the risk, or click on the link in the **Reference URL** field to be directed to the page in the IBM AI risk atlas for detailed information.



You can also click on a risk to open a new tab for it and review all the available fields. Finally, this view can be used to delete risks from the library if the client has their own curated list, or would like to build one from scratch. Risks can be imported via FastMap in a process similar to the one used to import business entities in the user management lab.

Now that you have reviewed the existing risks, you can proceed to creating your own.

2. Create a new risk

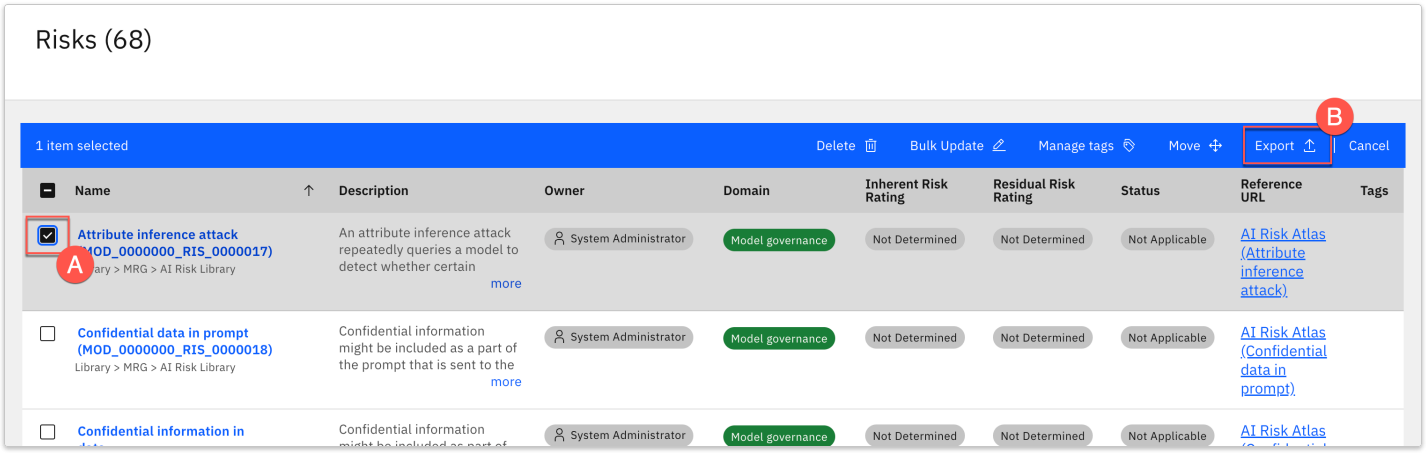
In this step, you will create a custom risk associated with agentic AI.

> At the time of writing, the risks in the risk library are stored in the governance console as children of a placeholder model created for this purpose.

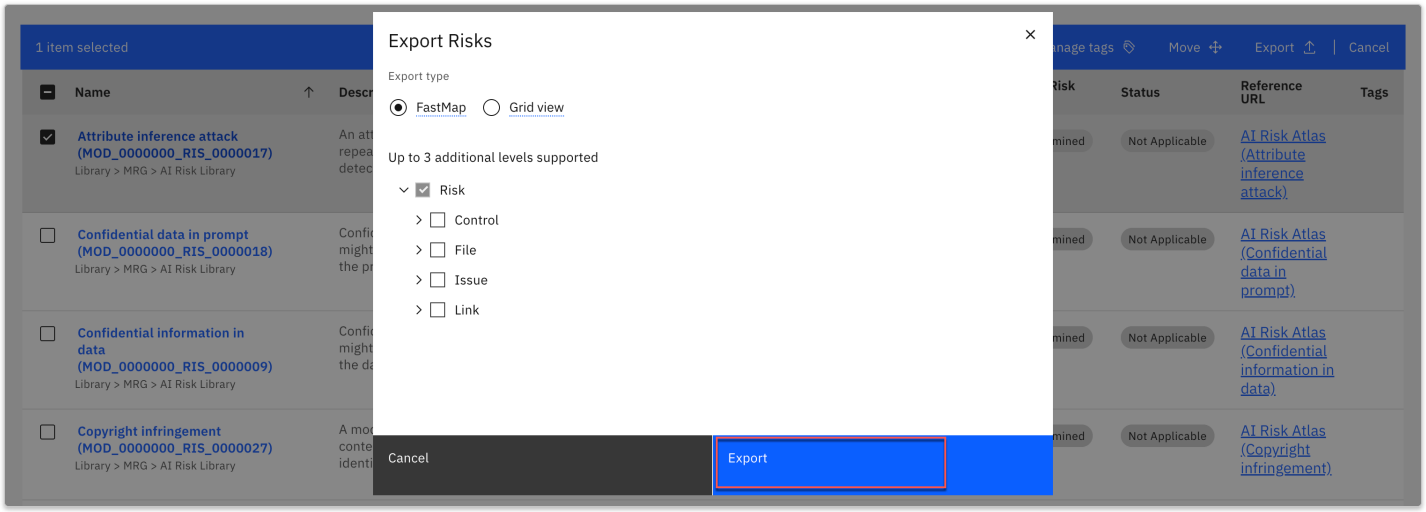
use the FastMap utility you explored in the user management lab.

FastMap import files must adhere to strict formatting requirements. The best method to ensure that your file meets these requirements is to export existing objects from the system and mimic that formatting for the objects you wish to add.

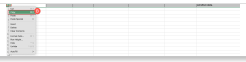
1. From the **Risks** table, check the box to the left of any one of the risk entries (A). Click on the **Export** button (B). The **Export Risks** window opens.



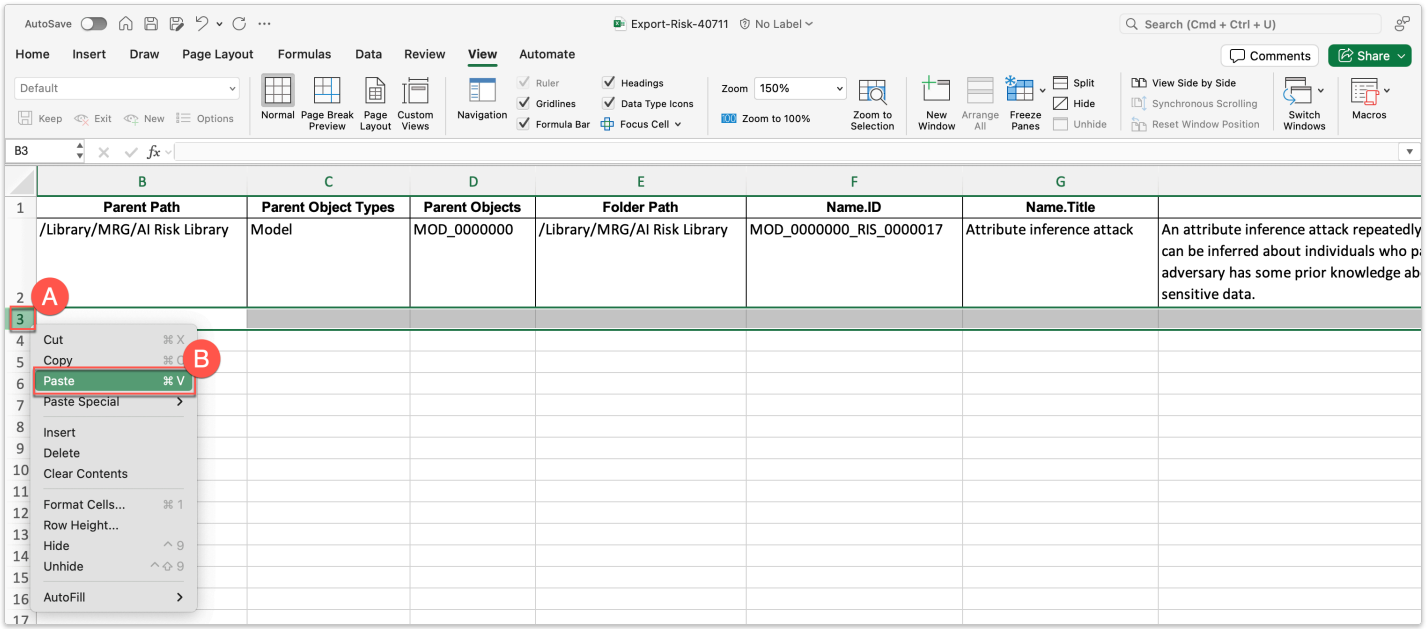
2. Click on the **Export** button. The export process runs, and you will be prompted to save the resulting file to your machine.



3. Open the spreadsheet on your machine. It will open to the **Risks** worksheet, which will contain a single line with the risk you selected when you performed the export.
4. Right-click on the index column for the existing risk (A) to select it and open the context menu. Click on the **Copy** item from the menu (B) to copy the row.

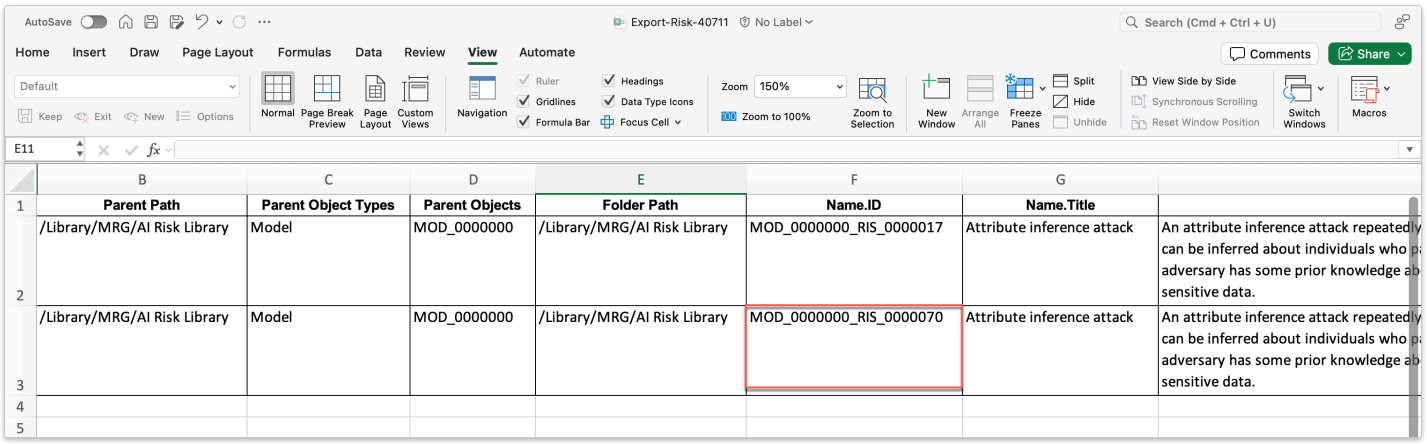


5. Right-click on the index column for the row **below** the existing risk (A) to select it and open the context menu. Click on the **Paste** item (B) from the menu to paste the information, duplicating the risk entry in the row beneath it.

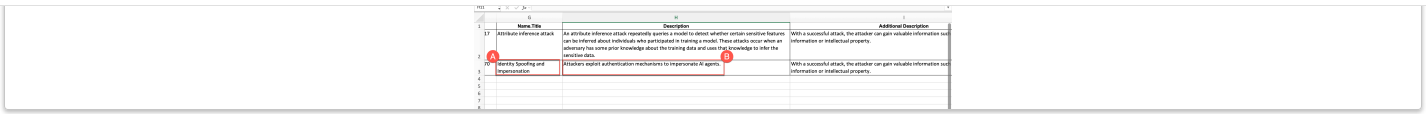


Your new entry now contains the correct fields in the correct format for importing into the governance console. You simply need to update some of the cells with information for your new risk.

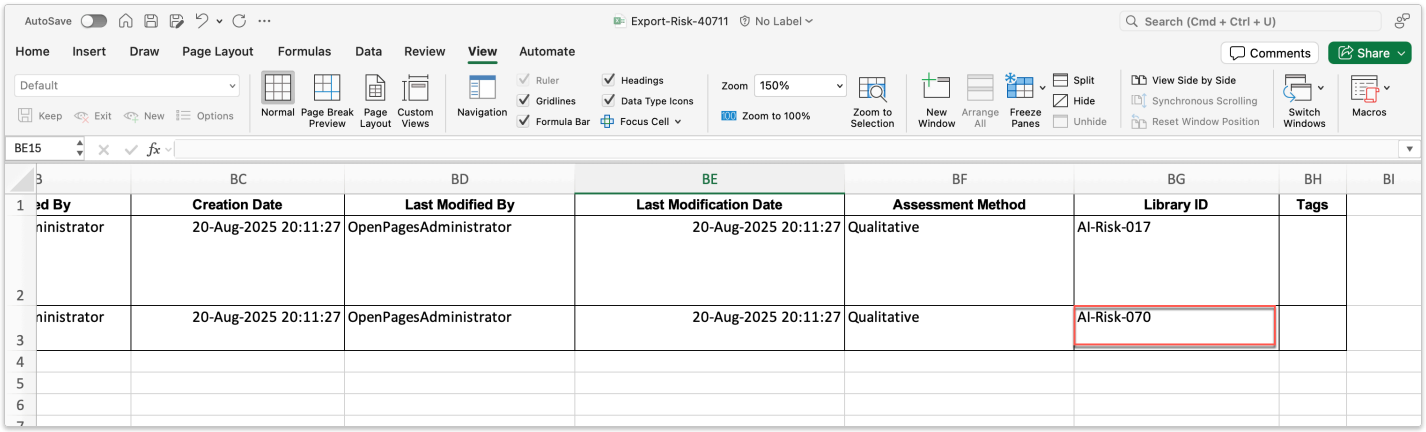
6. Locate the **Name.ID** column. This field is a unique identifier for the risk, and needs to be distinct from any other risks in the environment. The simplest way to make this unique is to increment the number at the end of the string beyond the number of risks in the library. For example, in the current environment, there are 68 risks (as seen when you opened the list of all risks), so you can update the **Name.ID** field from **MOD_0000000_RIS_0000017** to **MOD_0000000_RIS_0000070**.



7. Locate the **Name.Title** column (A) and enter **Identity Spoofing and Impersonation**. Locate the **Description** column (B) and enter **Attackers exploit authentication mechanisms to impersonate AI agents.**



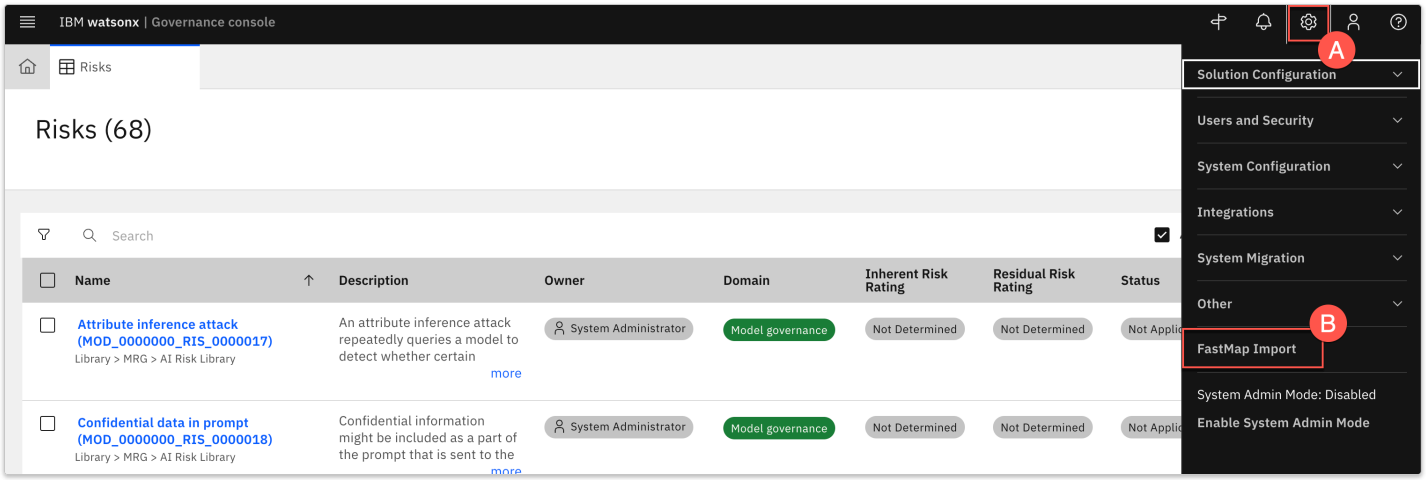
8. Scroll to the far right of the workbook and locate the **Library ID** column. Update it to match the number you assigned to the risk in step 6. If you followed the example in that step and used 70, then update the value to **AI-Risk-070**.



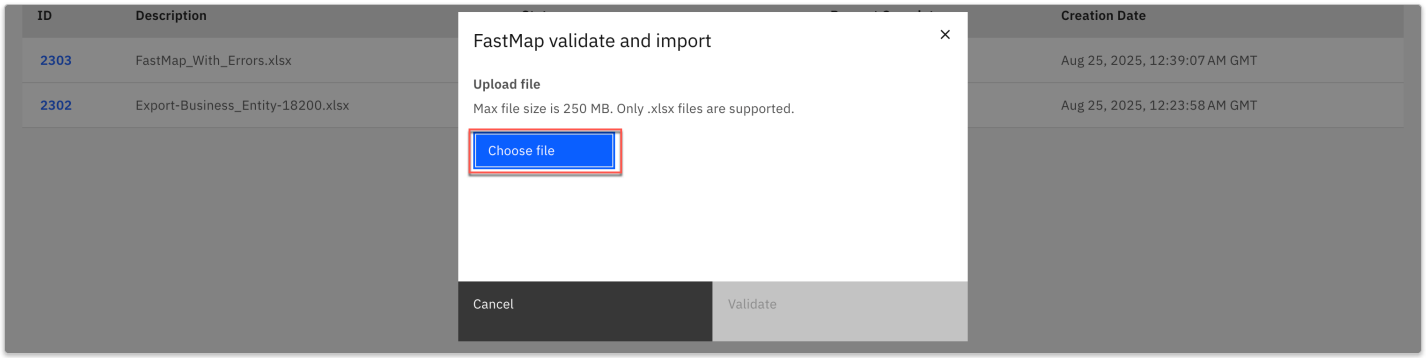
Name.ID	Creation Date	Last Modified By	Last Modification Date	Assessment Method	Library ID	Tags
ministrator	20-Aug-2025 20:11:27	OpenPagesAdministrator	20-Aug-2025 20:11:27	Qualitative	AI-Risk-017	
ministrator	20-Aug-2025 20:11:27	OpenPagesAdministrator	20-Aug-2025 20:11:27	Qualitative	AI-Risk-070	

At this point, you may take the opportunity follow steps 5-8 above to add any other risks you would like to your environment, adding each to a new line and specifying unique values for **Name.ID**, **Name.Title**, and **Library ID**.

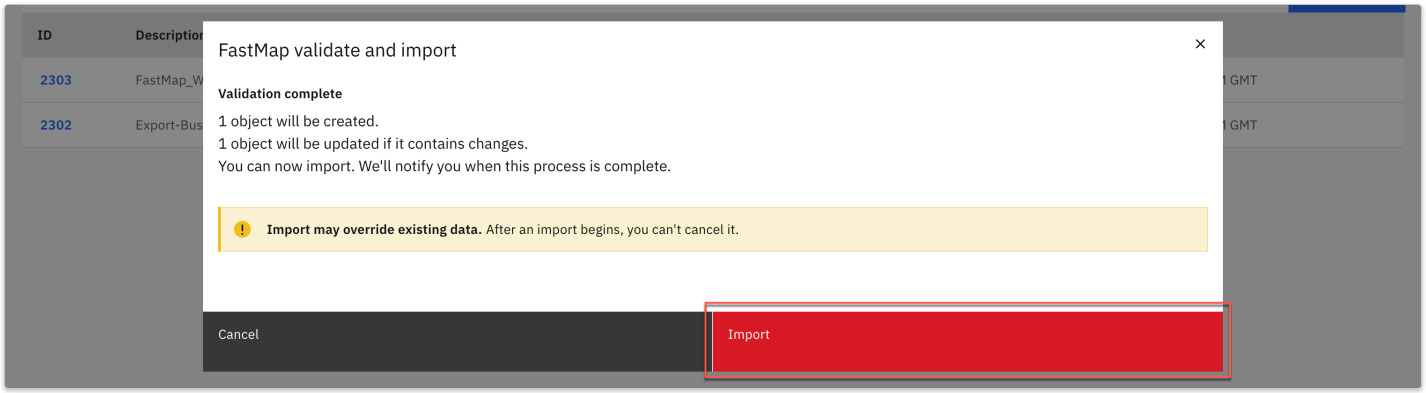
9. Save the changes to your spreadsheet file, and return to the watsonx governance console.
10. Click on the **gear icon** (A) to open the administration menu. Click on the **FastMap Import** menu item (B). A **FastMap Import** tab opens in your workspace.



11. Click on the **Import** button. The **FastMap validate and import** window opens.
12. Click on the **Choose file** button. You will be prompted to choose a file from your machine.



15. Click on the **Import** button to confirm your import. The **FastMap import details** window opens, tracking the progress of the import, which can take up to five minutes to complete.



16. Take a moment to review the import results, then click the **x** to close the **FastMap import details** window.
17. Click on the **Risks** tab in your workspace to return to it, and verify that the new **Identity Spoofing and Impersonation** risk is now in the table. Note that you can click on the risk from the table and edit any further details, such as providing a **Reference URL**.

You have successfully added a risk to the risk library, which can now be assigned to AI use cases either manually, or automatically via questionnaire. Next, you will explore mitigating controls.

Add a mitigating control

Controls are policies and procedures that make sure that risk mitigation responses are performed.

After you identify the risks that occur in your practices, establish controls, such as approvals, authorizations, and verifications. These controls remove, limit, or transfer these risks.

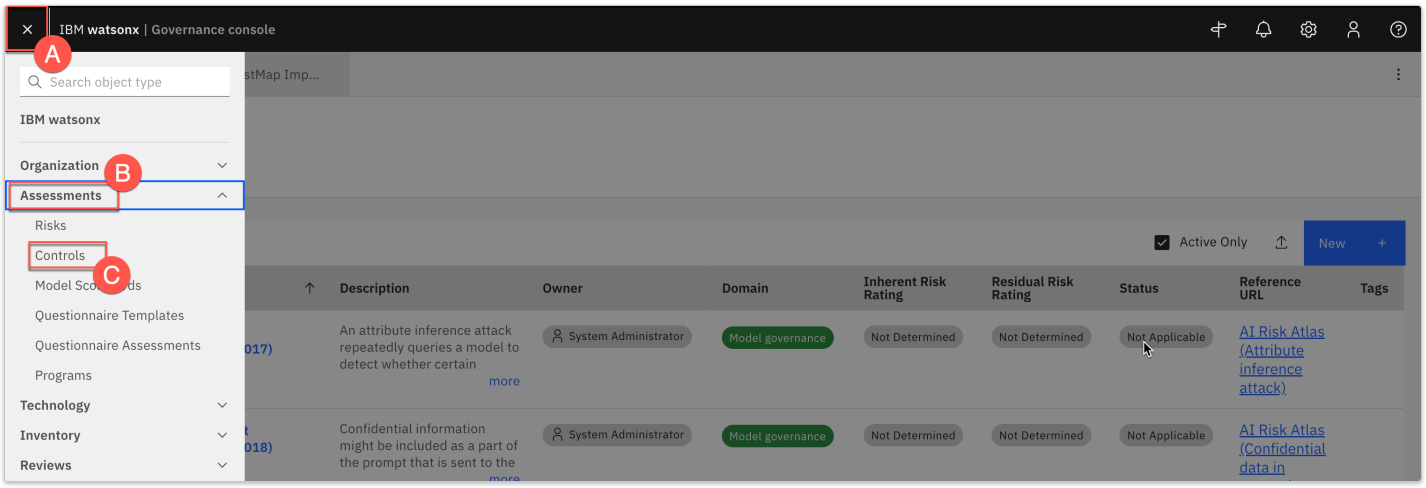
Controls provide either prevention or detection of risks. Controls are associated with tests that ensure that a control is effective. For example, AI models trained with unfairly biased training data frequently exhibit the same unfair bias during their operation.

In this lab, you will create a control for the **Identity Spoofing and Impersonation** risk you created in the previous section. A proper control for this risk would be to implement validation frameworks and boundaries to detect impersonation attempts.

1. Create a control

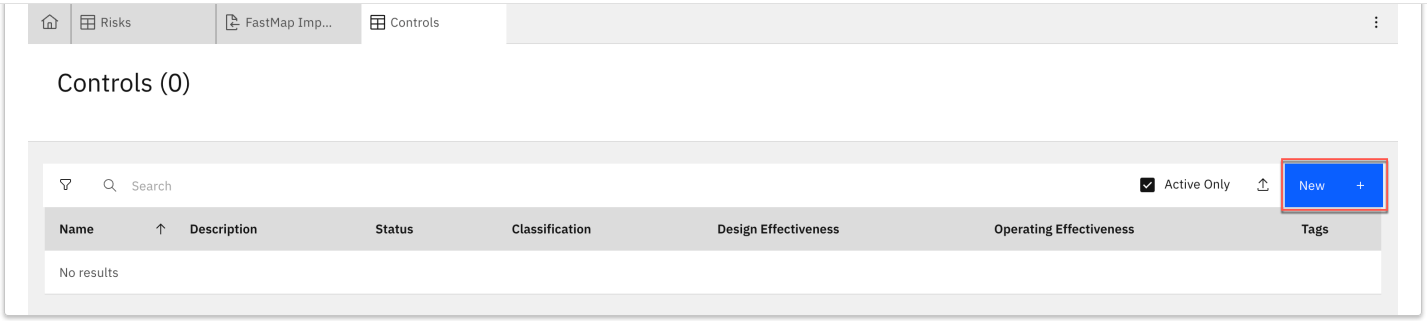
Controls are treated as objects in the governance console, and contained in the inventory with questionnaires and assessments.

1. Click on the **menu button** in the upper left (A) to open the menu. Click on the **Assessments** menu item (B) to expand it. Click on the **Controls** menu item (C). The **Controls** tab opens.

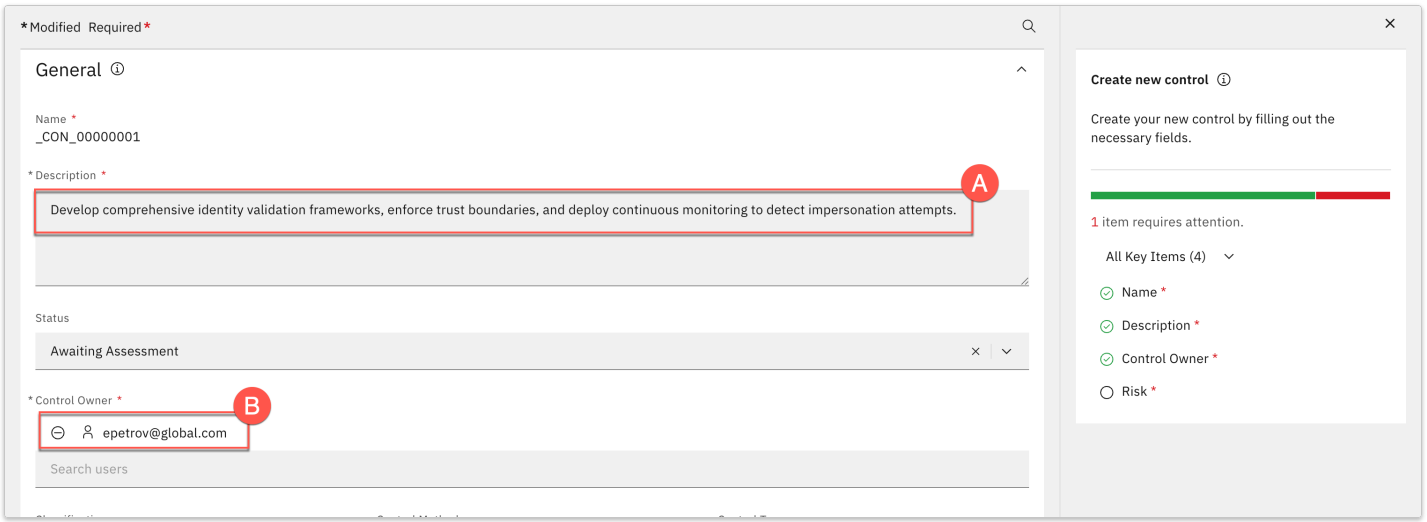


At the time of writing, no existing controls are provided by default. As with other objects in the governance console, you can create multiple controls at once using a FastMap import. For this lab, you will create a control with the user interface.

2. Click on the **New** button. A **New Control** tab opens in your workspace.

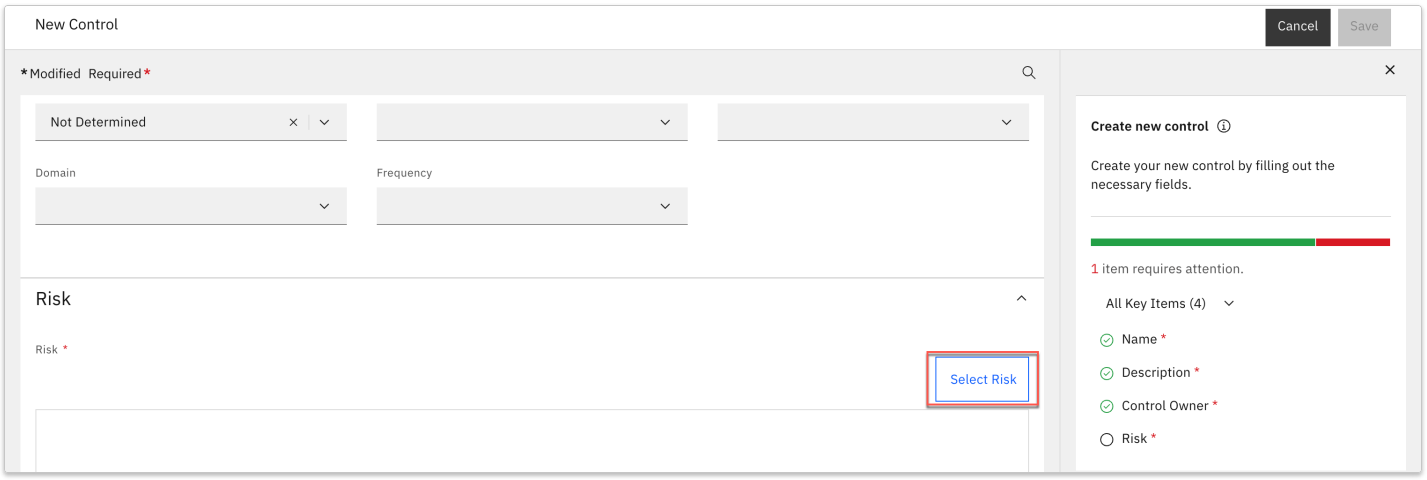


3. In the **Description** field (A), enter the following text: *Develop comprehensive identity validation frameworks, enforce trust boundaries, and deploy continuous monitoring to detect impersonation attempts.* Click on the **Control Owner** field (B) and enter the **epetrov@global.com** user. Recall that this user is Elena Petrov, a DevOps specialist in the Information Technology department, who would own the identity valuation frameworks.

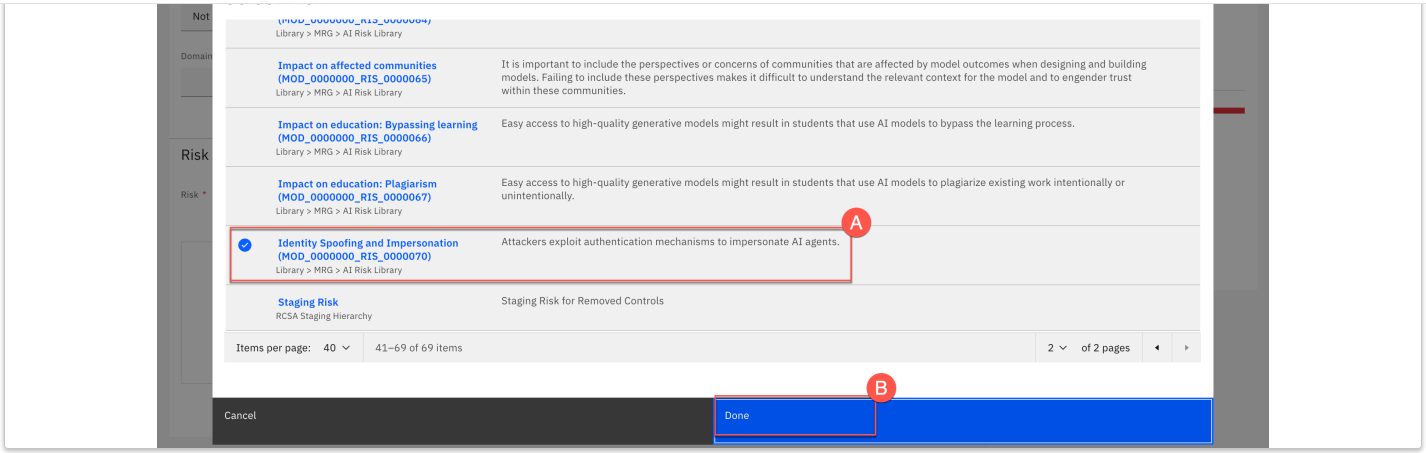


Next, you will associate this control with a specific risk.

4. Scroll down to the **Risk** section and click on the **Select Risk** button. The **Select Risk** window opens.



5. Locate the **Identity Spoofing and Impersonation** risk you created in the table (A) and click on it to select it. Note that you may need to use the buttons at the bottom of the table to move to the second page. Click on the **Done** button (B) to confirm your selection. The **Select Risk** window closes.



6. Click on the **Save** button to save your control.

You have now created a mitigating control associated with your risk. Organizations can use defined controls to ensure that risk mitigation efforts are properly documented, and can make them part of their approval workflows. Note that at the time of writing, controls are not automatically assigned to use cases when risks are identified, and must be manually added.

Create a questionnaire for risk evaluation

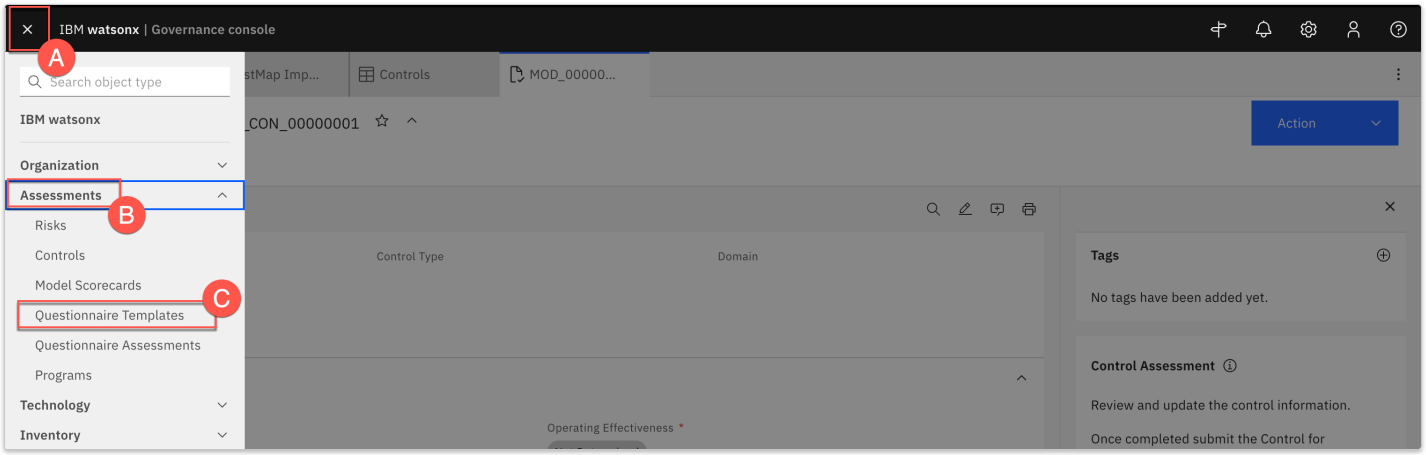
Questionnaires provide a valuable tool for stakeholders and subject matter experts to evaluate their use case requests for potential risks. The watsonx governance console contains a detailed questionnaire as part of the default workflow; relevant risks from the default risk library are automatically added to the use case based on answers in the form.

Many clients may choose to use this default questionnaire as a starting point, customizing it as necessary. For the purposes of this lab, you will create a new questionnaire from scratch to address the risk you added in previous sections, but the instructions could be easily adapted to simply add the related questions to the existing questionnaire.

1. Create a new questionnaire template

Questionnaires that can be created and attached to use cases are referred to in the governance console as questionnaire templates.

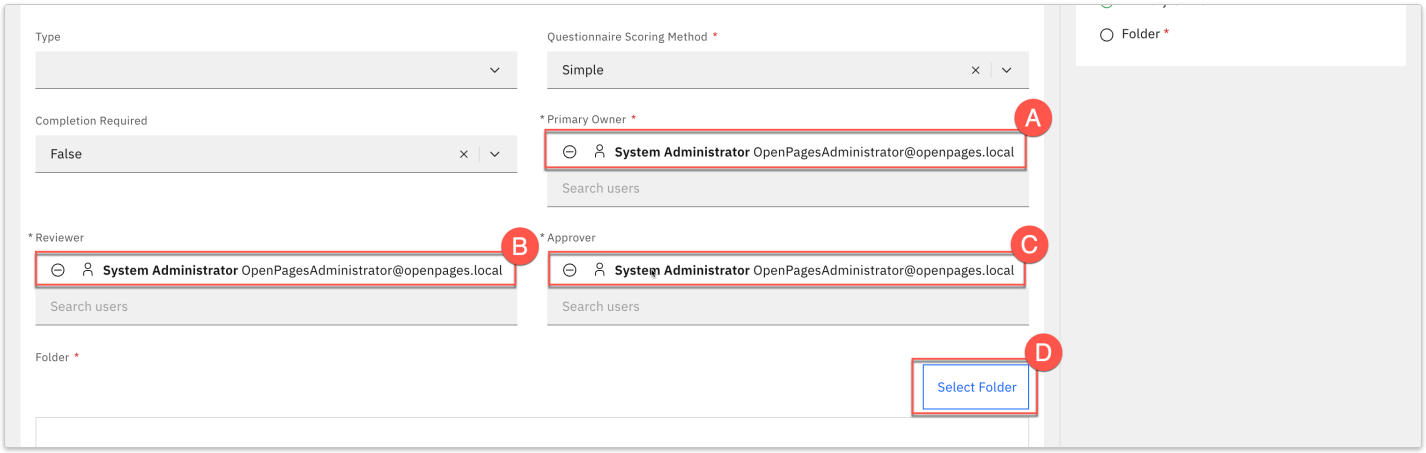
1. Click on the **primary menu** button in the upper left (A) to open the menu. Click on the **Assessments** menu item (B) to expand it. Click on the **Questionnaire Templates** menu item (C). A **Questionnaire Templates** tab opens in your workspace.



Four pre-defined templates are available, including the **AI Risk Identification Questionnaire** discussed above, and the **EU AI Act Applicability Assessment**, which is designed to help determine if the EU AI Act applies to the requested use case. Examining the construction of these questionnaires can help provide a sense of the different capabilities available, beyond those discussed in this lab.

2. Click on the **New** button. A **New Questionnaire Template** tab opens in your workspace.
3. Enter **Custom Risk Identification Questionnaire** in the **Name** field (A). Enter **Sample questionnaire for agentic AI risks** (B) in the **Description** field.

4. Click on the **Primary Owner** field (A) and select the **System Administrator** user. Click on the **Reviewer** field (B) and select the **System Administrator** user. Click on the **Approver** field (C) and select the **System Administrator** user. Click on the **Select Folder** button (D). The **Select Folder** window opens.



5. Scroll down to the **Library** folder in the table and click on it to select it.

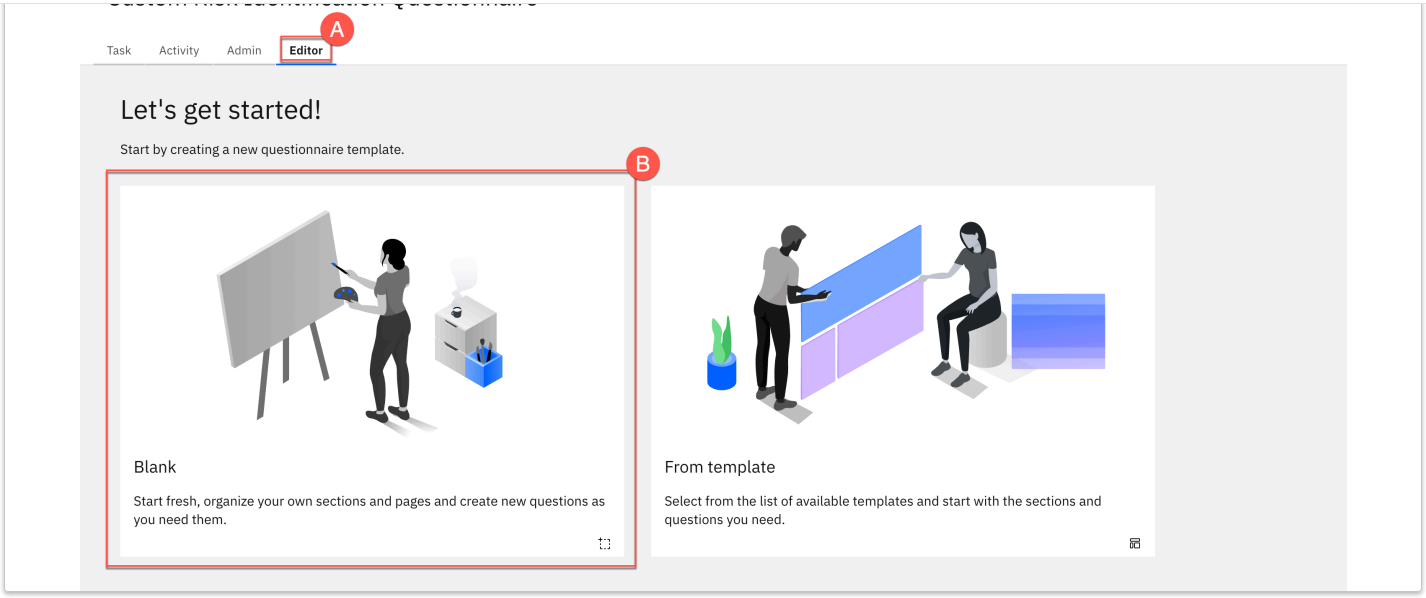
12. Click on the **Done** button to save your selection and close the **Select Folder** window.
13. All the required fields have been populated; click on the **Save** button to save your changes. The screen changes to the **Task** view for the questionnaire assessment.

Next, you will add questions to the template.

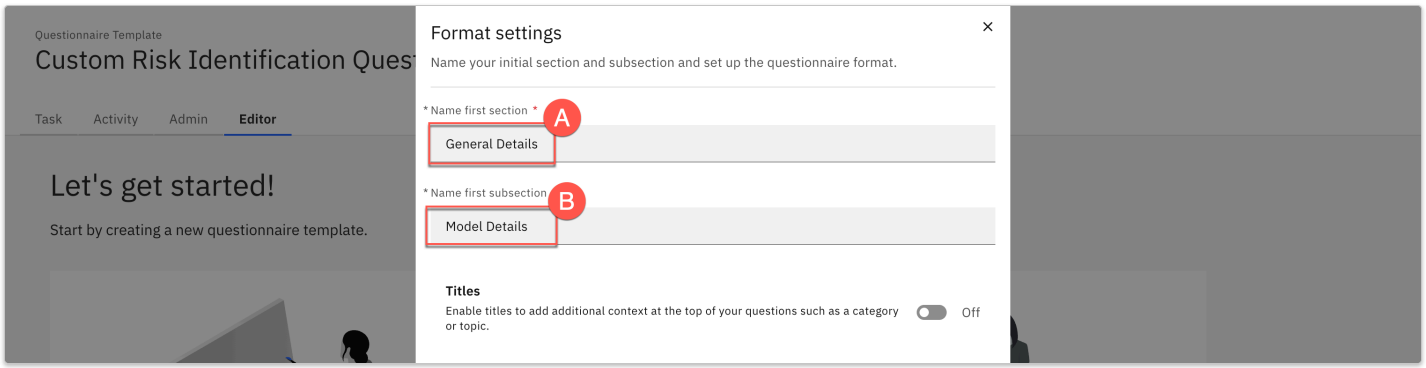
2. Add a question

When creating a questionnaire, you can start from a blank form, or you can start with a template. In this lab, you will begin with a blank form.

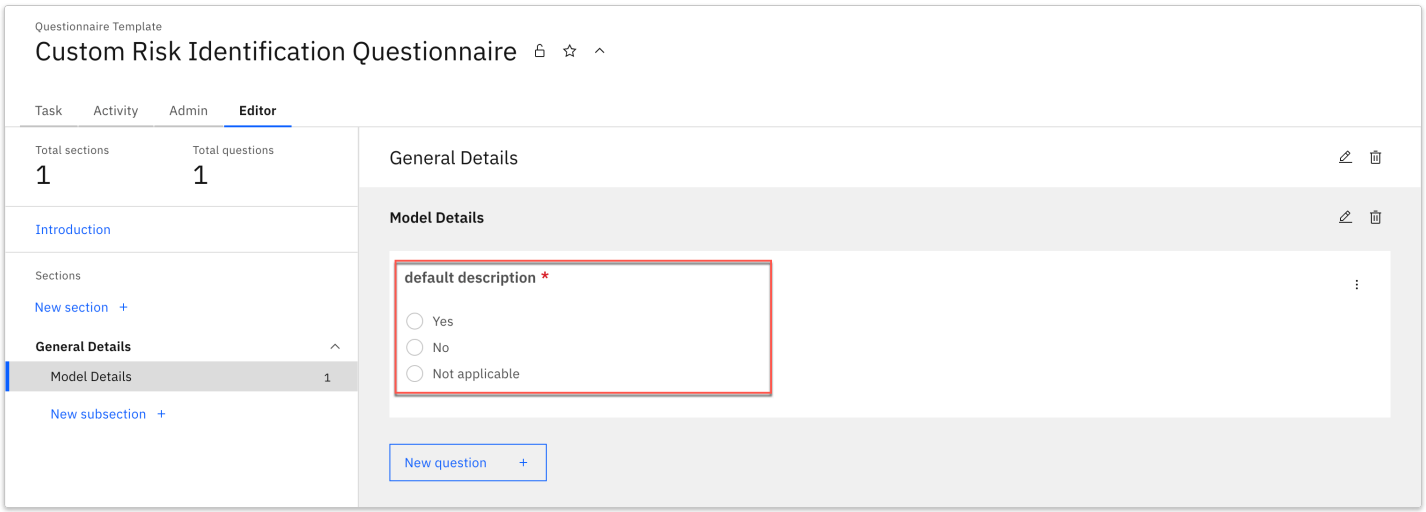
1. From the **Task** view, click on the **Editor** tab (A) to switch to it. Click on the **Blank** tile (B). The **Format settings** window opens.



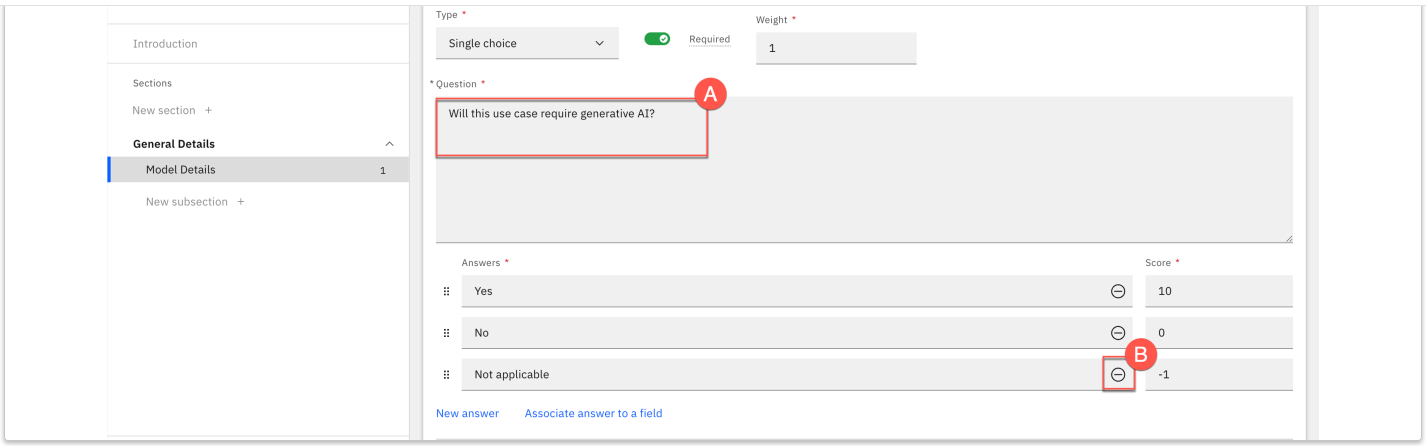
2. Enter a name like *General Details* in the **Name first section** field (A). Enter a name like *Model Details* in the **Name first subsection** field.



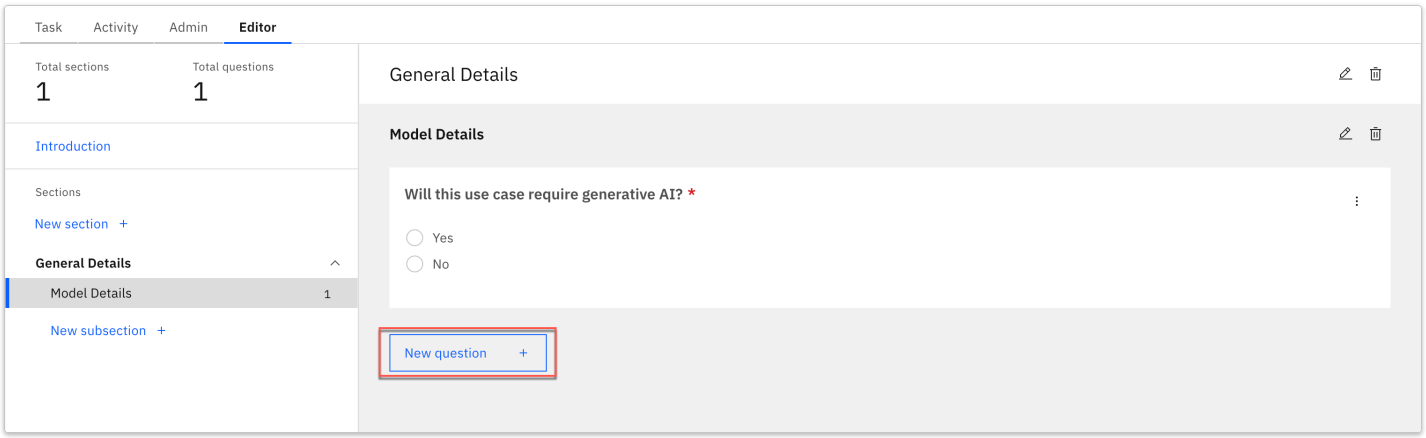
3. Click on the **Create** button. The **Format settings** window closes and the questionnaire editor opens with a default placeholder question loaded.
4. Click on the tile for the placeholder question to edit it. The **Configure question** tile opens.



5. Enter **Will this use case require generative AI?** in the **Question** field (A). Click on the **Remove** button for the **Not applicable** answer (B), since you do not want to provide this as an answer option.



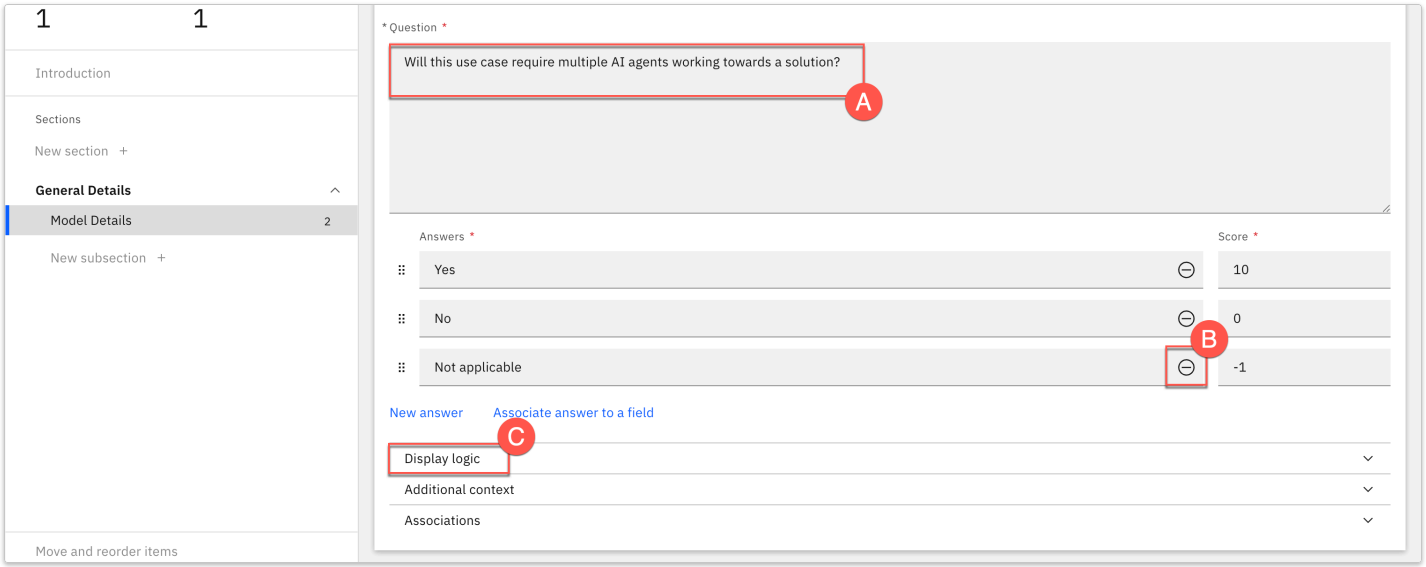
6. Click in the gray area above the **Configure question** tile to finalize your changes. Changes to the questionnaire template are automatically saved after each change.
7. Click on the **New Question** button. Another **Configure question** tile opens.



8. Enter **Will this use case require multiple AI agents working towards a solution?** in the **Question** field (A). Once again, click on the **Remove** button (B) for the **Not applicable** answer.

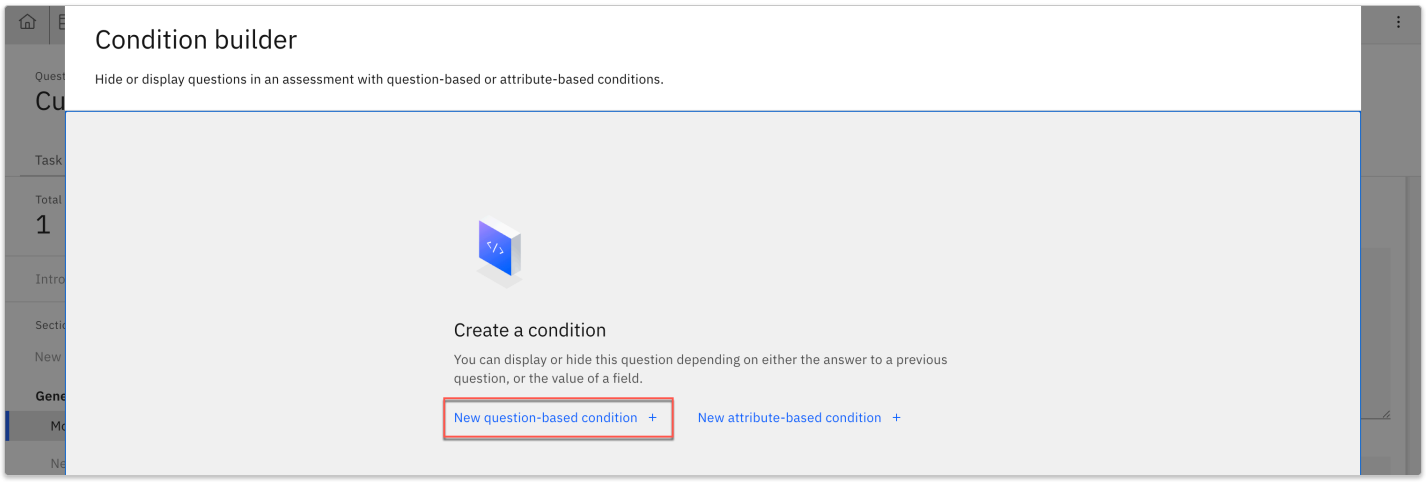
This question should only be presented to the user if they answered **Yes** to the previous question about using generative AI. You will now modify the question's display logic to reflect this.

Click on the **Display logic** section header (C) to expand it.

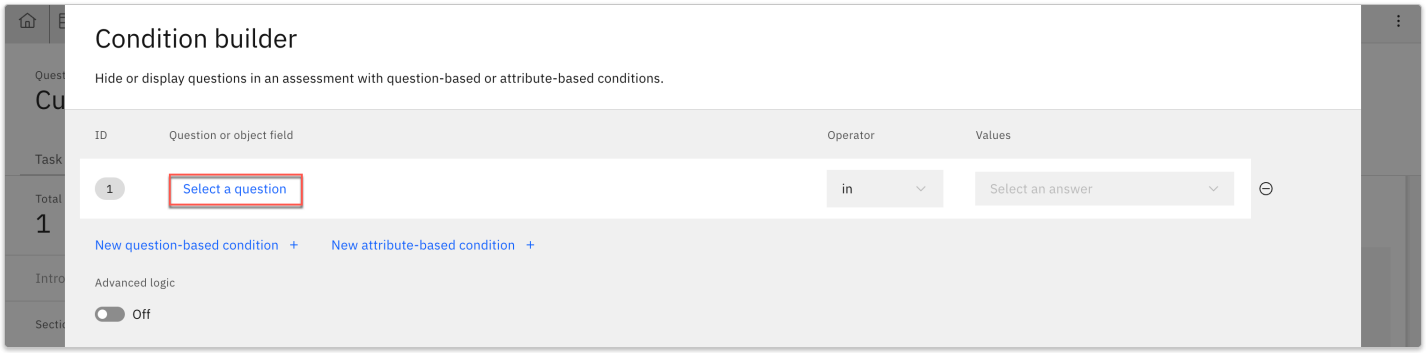


9. Click on the **Condition builder** button in the **Display logic** section. The **Condition builder** window opens.

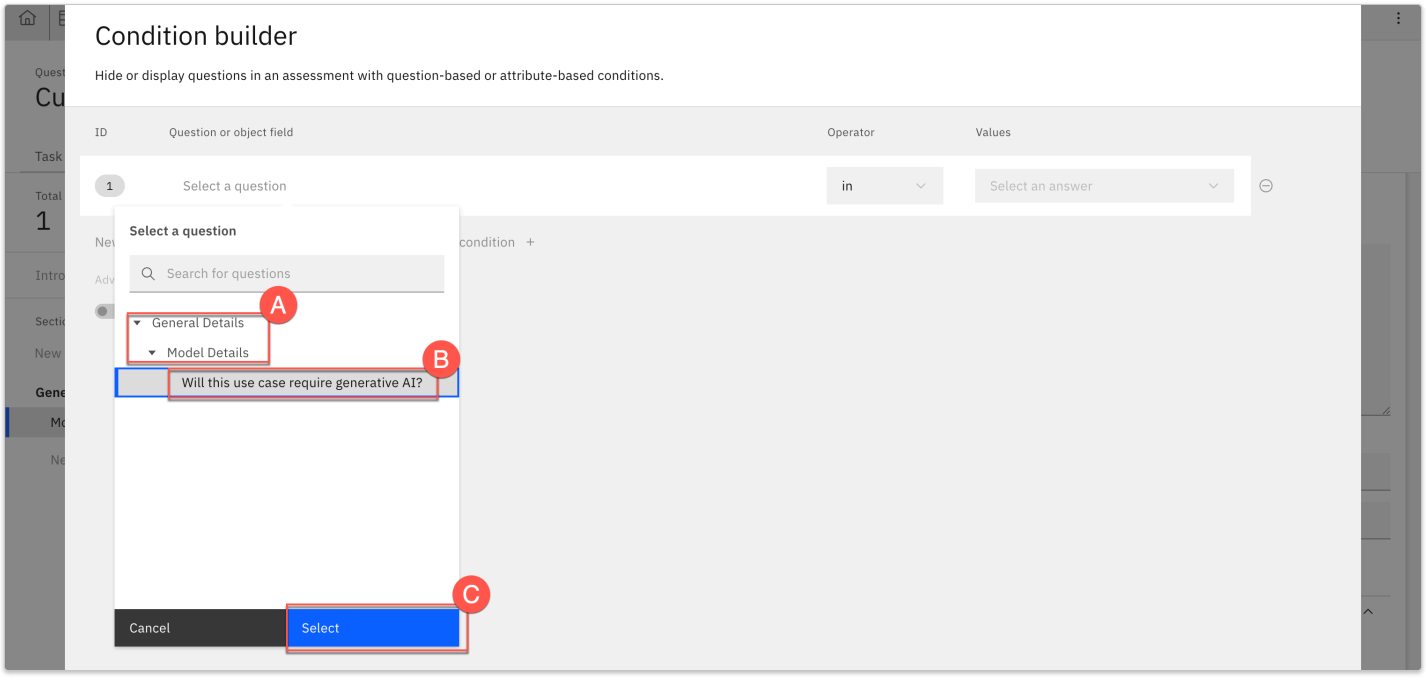
10. For this question, click on the **New question-based condition** button.



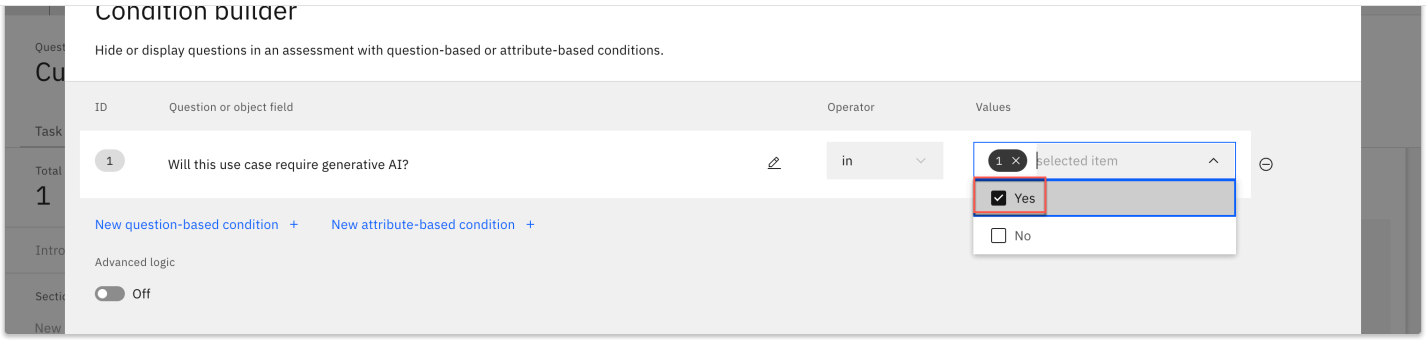
11. Click on the **Select a question** button to identify the question you would like to use to determine the display logic.



12. Click on the sections (A) to expand them until the **Will this use case...** question is available, then click on it (B) to select it. Click on the **Select** button (C) to confirm your choice.



13. Click on the **Values** field and check the box next to **Yes** to indicate that you want to display the question about AI agents if the generative AI question has been answered with a *Yes*.



Note that you can add as many conditions as are appropriate for each question.

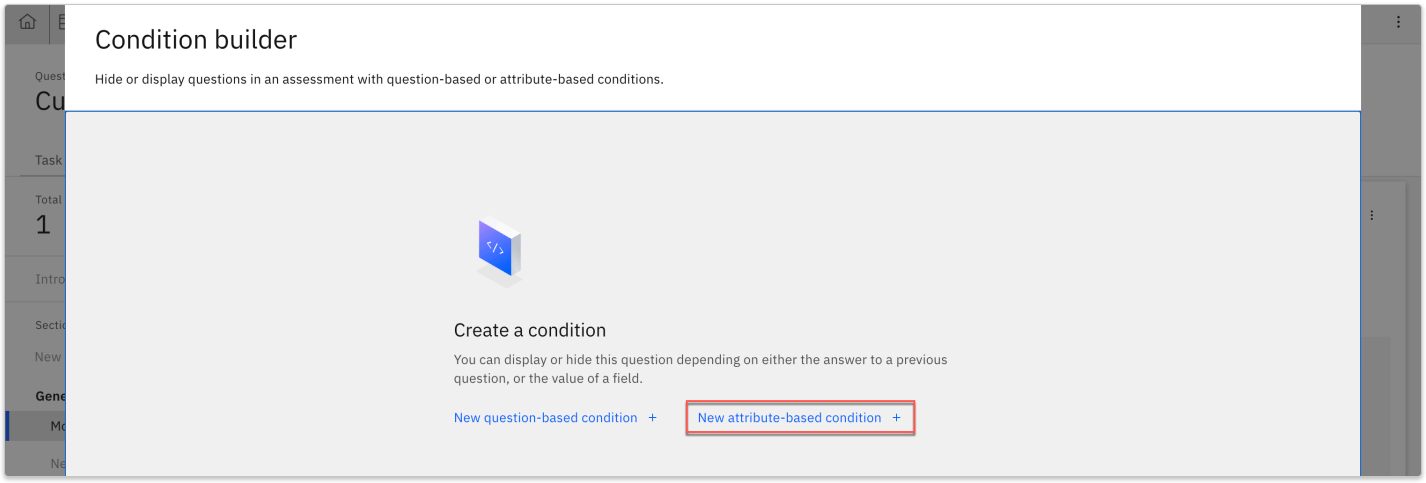
14. Click on the **Save** button to save the condition. The **Condition builder** window closes.
15. Click in the gray area above or below the **Configure question** tile to save your changes to the question. Note that a small icon appears above the question text, denoting that the question has custom display logic.

Next, you will create a question with attribute-based display logic.

3. Add a second question

As mentioned above, questions can also be hidden or displayed based on attributes of the use case they relate to. For example, you may wish to ask for specific details and context if the model will be accessing data related to human resources.

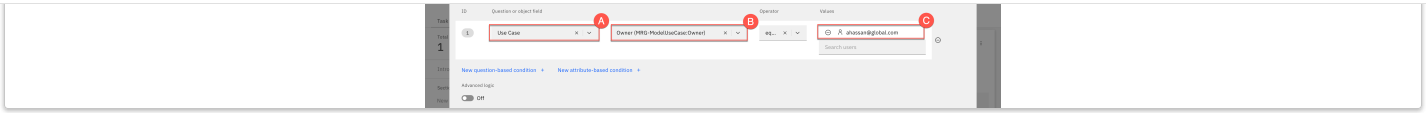
1. Click on the **New question** button. A **Configure question** panel opens.
2. Enter **Will the model need access to personal identifiable human resources data?** in the **Question** field.
3. Click on the **Remove** button for the **Not applicable** answer.
4. Click on the **Display logic** section header to expand it.
5. Click on the **Condition builder** button to open the condition builder.
6. Click on the **New attribute-based condition** button.



You will use the condition builder to specify that this question be asked if the use case is owned by the human resources department.

7. Click on the **Choose an object** dropdown (A) to open it, and click on the **Use Case** item to select it. Click on the **Choose a field** dropdown (B) to open it, and click on the **Owner...** item to select it.

Click on the **Search users** field (C) and enter the **ahassan@global.com** user. Recall that this user is Aisha Hassan, manager of the Human Resources department. Note that in a real-world use case, you would likely have created a group of Human Resources managers, then used that group in this display logic. Also note that you can specify multiple valid owners to satisfy the condition if necessary.

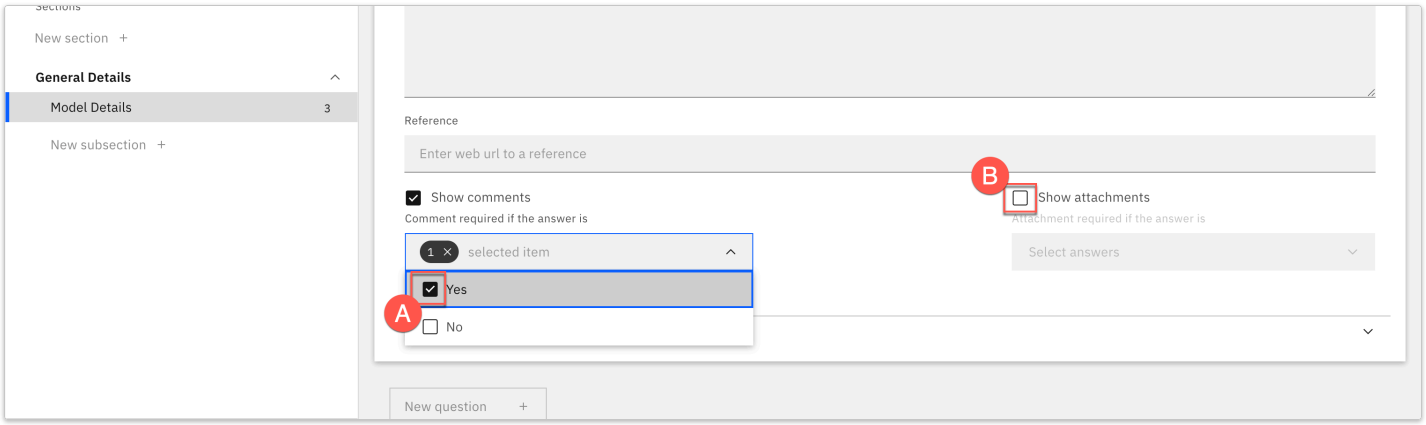


8. Click on the **Save** button to save the condition and close the **Condition builder** window.

You have set the display conditions for the question, but it would be useful if the question prompted the user for more context if they answered *Yes*.

9. Click on the **Additional context** section header to expand it.

10. Scroll to the **Comment required if the answer is** item on the form, and click on the **Select answers** dropdown (A). Check the box next to the **Yes** answer to select it. Uncheck the box to the left of **Show attachments** (B) to deselect it, as you will not require file attachments for this question.



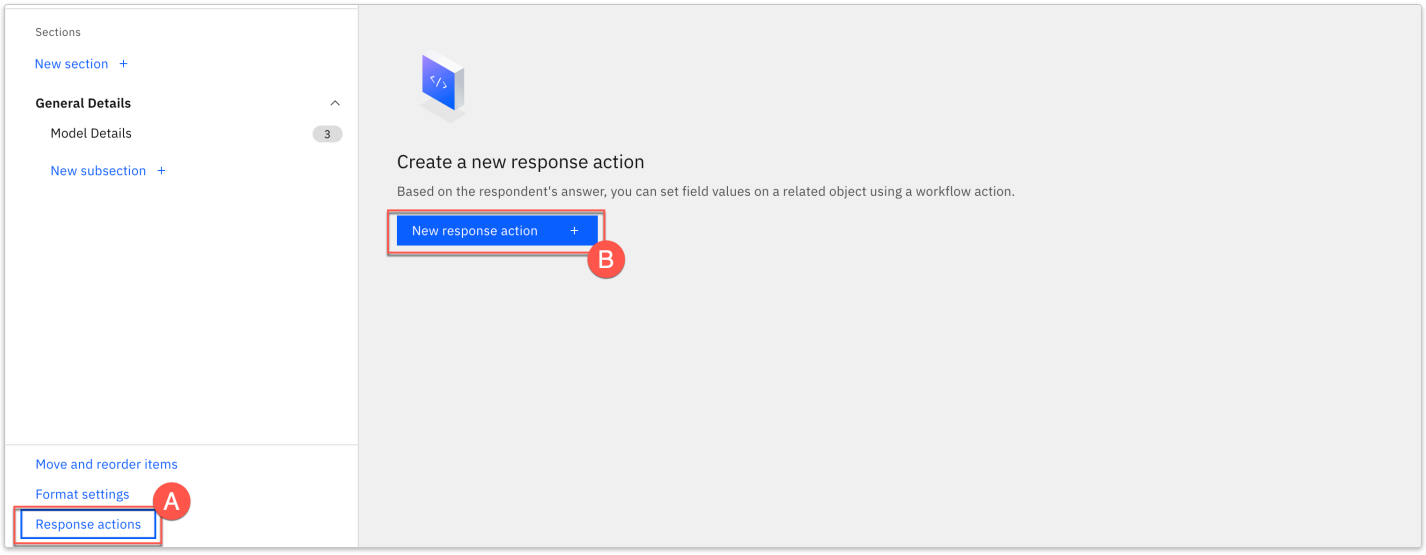
11. Click in the gray area above or below the **Configure question** tile to save your changes to the question.

You have experimented with the logic for displaying questions in a questionnaire. Next, you will use the answers to the questions to associate relevant risks from the risk library.

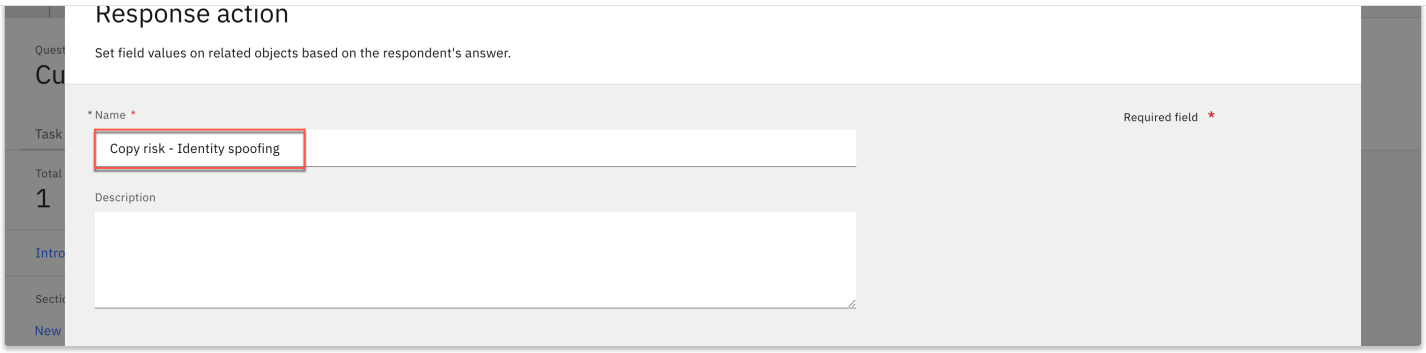
4. Add response actions

Response actions are used to modify objects based on the answers to questions. In this case, you will use them to attach relevant risks to the use case associated with the questionnaire.

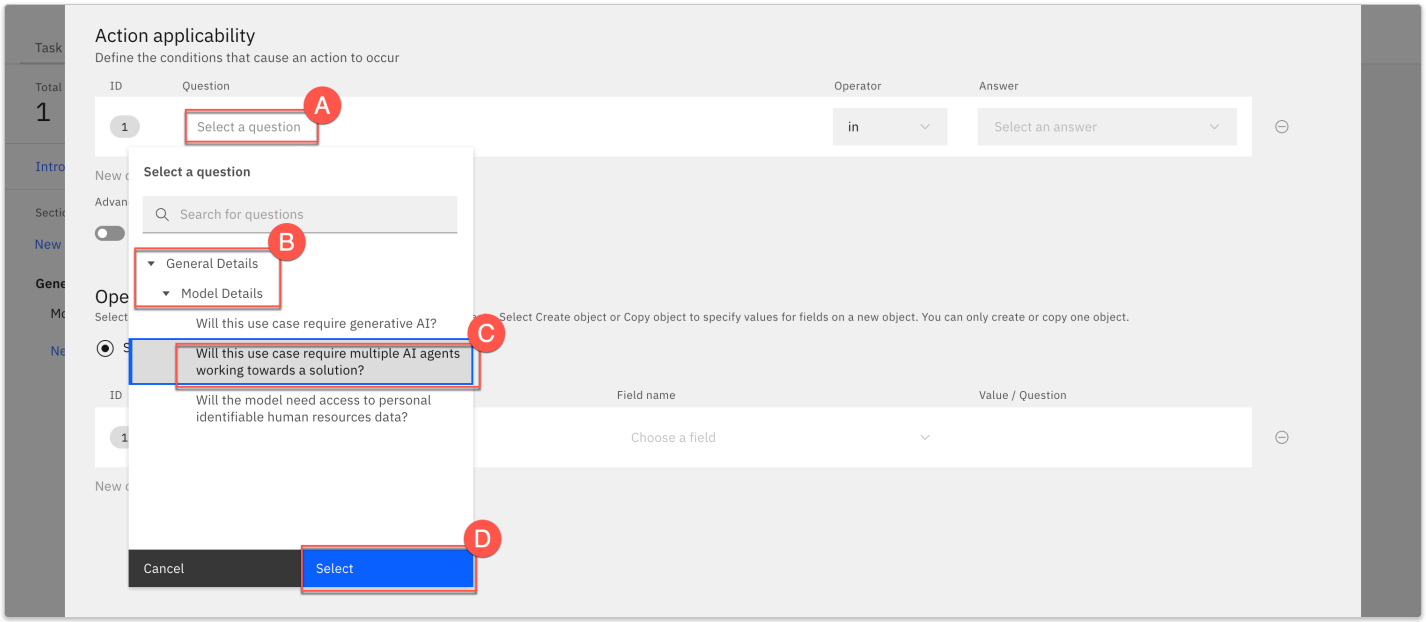
1. Click on the **Response actions** button in the lower left (A). The **Create a new response action** section opens. Click on the **New response action** button (B). The **Response action** window opens.



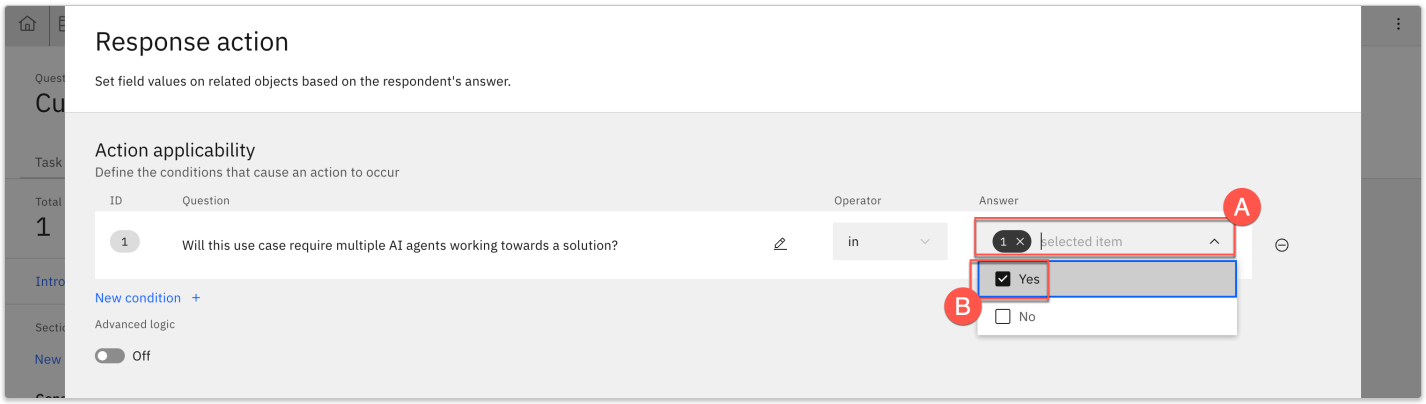
2. Enter **Copy risk - Identity spoofing** in the **Name** field.



3. Scroll down to the **Action applicability** section and click on the **Select a question** button (A). Expand the sections (B) until the **Will this use case require multiple AI agents...** question is available, then click on it (C) to select it. Click on the **Select** button (D) to confirm your choice.



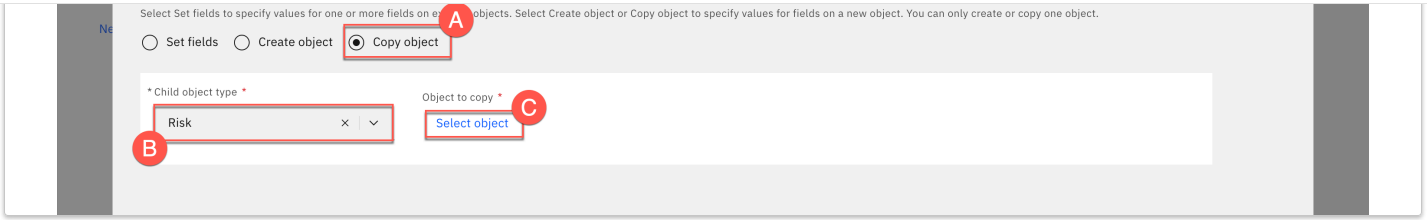
4. Click on the **Answer** dropdown (A) to expand it. Check the box next to **Yes** (B) to indicate that you want the action to occur if the answer was *Yes*.



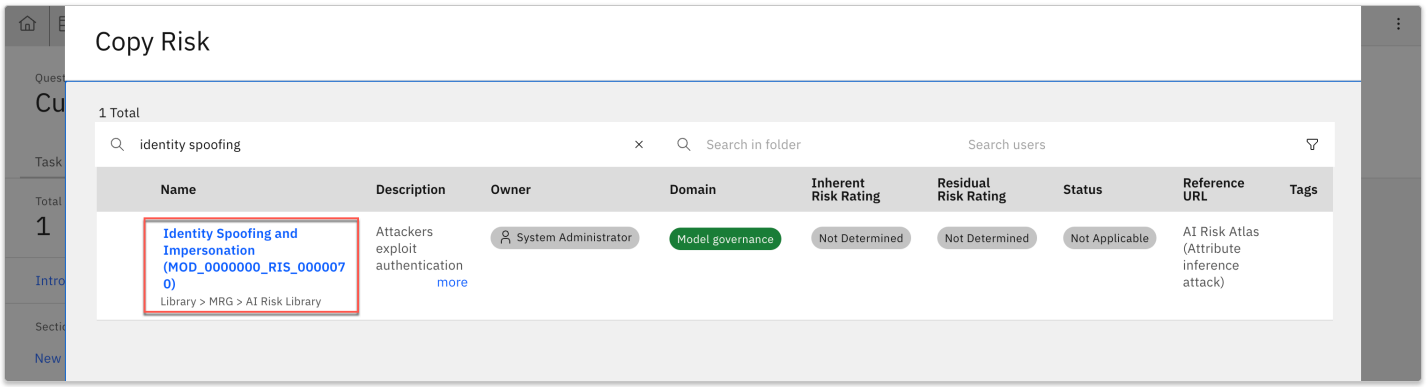
Note that you can use the **Advanced** logic field to work with multiple conditions using boolean logic if necessary.

> In the watsonx governance console, risks are assigned to use cases by creating a copy of the risk object from the risk library as a child object of the use case.

5. Scroll down to the **Operations** section and select the **Copy object** option (A). Click on the **Child object type** dropdown and select **Risk** (B). Click on the **Select object** button beneath **Object to copy** (C). The **Copy Risk** window opens.



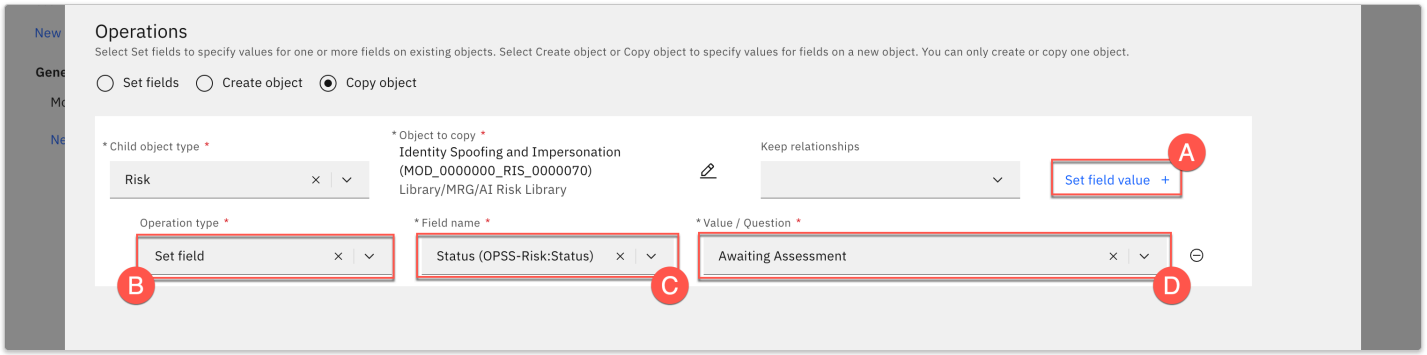
6. Locate the **Identity Spoofing...** risk in the table and click on it to select it. Note that you can use the **Search** bar to narrow the list to quickly locate the applicable risk.



7. Click on the **Done** button to confirm your choice and close the **Copy Risk** window.

You can also use the response action to set a field for the risk. In this case, you will set the risk to **Awaiting assessment** so that the risk management officers can evaluate it.

8. Click on the **Set field value** button (A). Click on the **Operation type** dropdown to open it, and select **Set field** (B). Click on the **Field name** dropdown to open it, and select **Status...** (C). Click on the **Value / Questions** dropdown, and select **Awaiting Assessment** (D).



9. Click on the **Save** button to save your response action and close the **Response action** window.

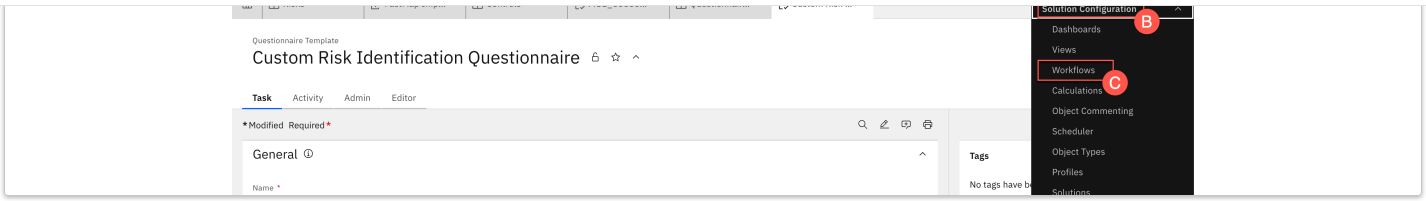
If you wish, you can use similar steps to assign risks based on answers to the other questions. For example, you could associate the risk of personally identifiable information (PII) leakage for the human resources model question.

Now that you have created the questionnaire, you need to ensure that it will be used in the AI use case request workflow.

5. Replace the existing questionnaire

The watsonx governance console provides a default workflow for AI use case evaluations, which includes the risk identification questionnaire. In order for your new custom questionnaire to be included, you must modify the default workflow. In this section you will briefly work with it to make the change. The next lab will cover workflows in much greater depth.

1. From the governance console, click on the **gear icon** (A) to open the administration menu. Click on the **Solution Configuration** menu item (B) to expand it. Click on the **Workflows** menu item (C). The **Workflows** tab opens in your workspace.

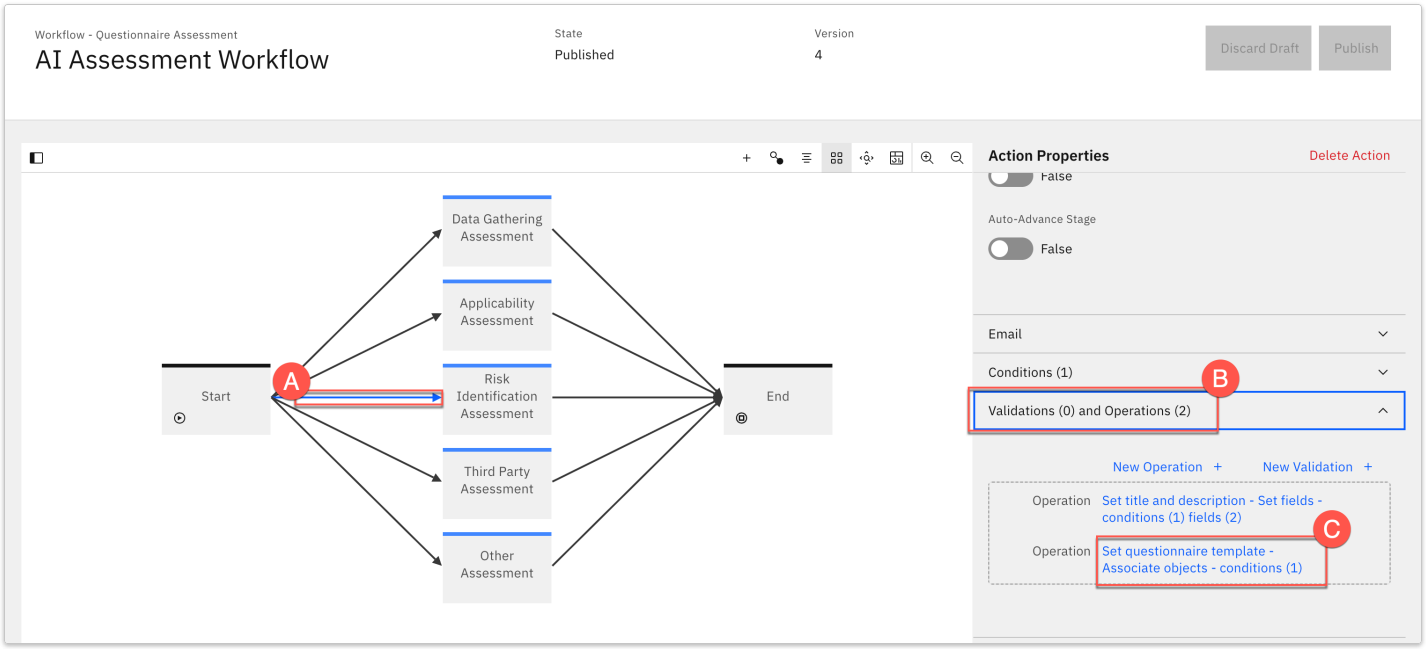


You can ignore the warning about your current profile not having access to all the views on the page.

2. Locate and click on the **AI Assessment Workflow** from the table. A new tab showing the workflow opens in your workspace.

Workflows consist of stages, represented by the boxes, and actions, represented by the arrows between the stages. For this step, you will need to modify the action effecting the risk identification assessment after the use case process has started.

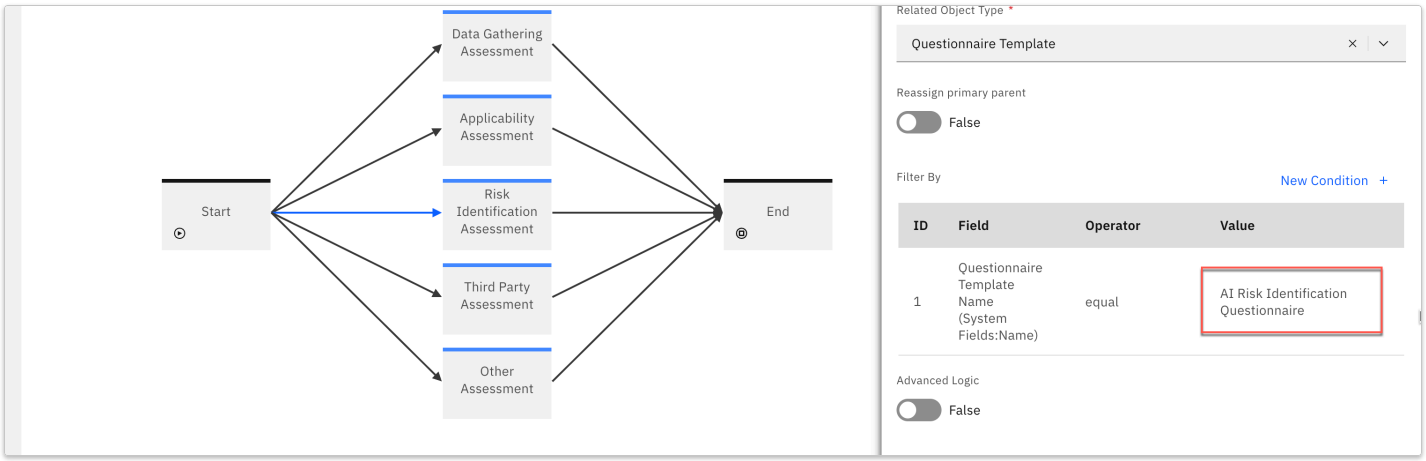
3. Locate and click on the **arrow** between the **Start** stage and the **Risk Identification Assessment** stage (A). The **Action Properties** panel opens. In the **Action Properties** panel, click on the **Validations and Operations** section header (B) to expand it. Click on the **Set questionnaire template...** operation (C). The **Operations** panel opens.



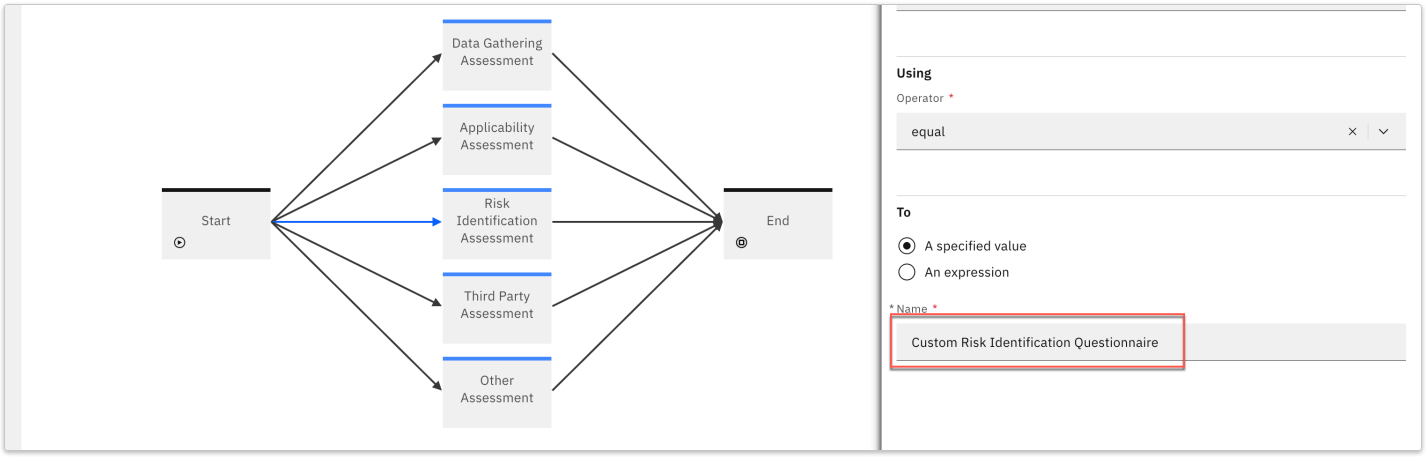
The next lab will provide more detail on the different settings for operations. For now, you will simply change the governance console object that is being associated with this particular step of the workflow.

4. Click on the **Edit** button next to the **Object to associate** field. The **Object to associate** panel opens.

5. Click on the **AI Risk Identification Questionnaire** in the **Filter By** table. The **Filter By** panel opens.



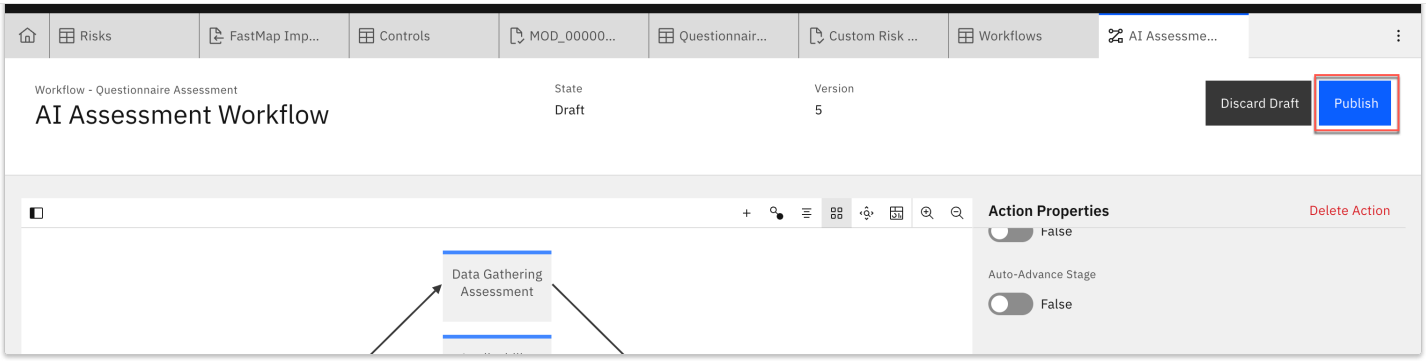
6. Enter **Custom Risk Identification Questionnaire** in the **Name** field. Note that this name must **EXACTLY** match the name you used for your questionnaire, as the system will use that string to search existing questionnaires when finding the object to associate with the use case as it progresses through the workflow.



7. Click on the **Done** button to close the **Filter By** panel.
8. Click on the **Done** button again to close the **Object to associate** panel.
9. Click on the **Done** button again to close the **Operations** panel.

The **Publish** button will be disabled as your workflow changes are automatically saved. When the system is finished saving the changes, the **Publish** button becomes enabled once again.

14. Click on the **Publish** button to publish your changes.



You have now integrated your questionnaire into the default AI use case request workflow.

Conclusion

In this lab, you explored risks, controls, and questionnaire templates. You examined the default risk library in the watsonx governance console, and added a risk relevant to agentic AI. You then created a mitigating control for that risk. Finally, you created a custom risk assessment questionnaire template to evaluate use cases for the risk you created.