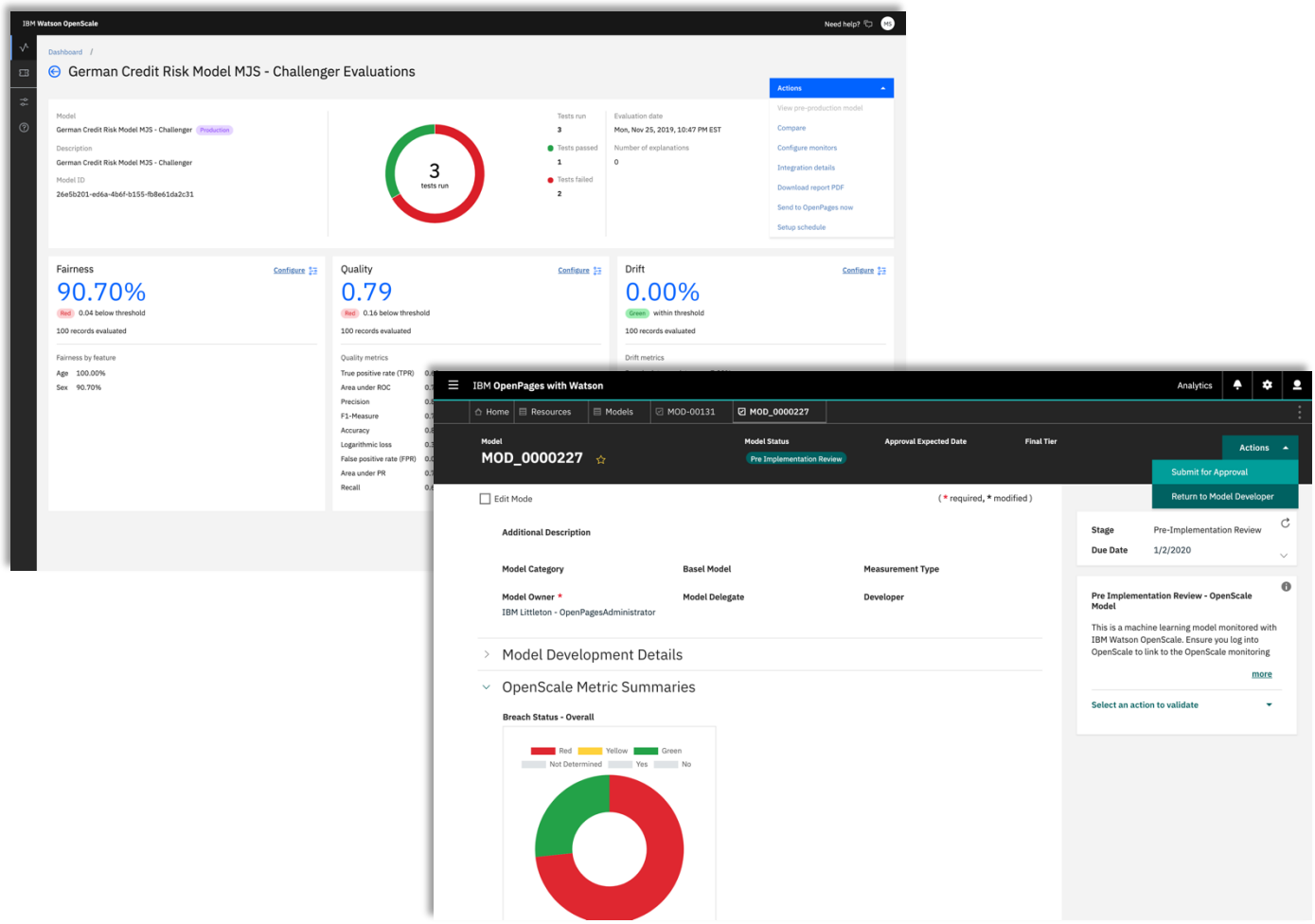
Model Risk Management with IBM Watson OpenScale and IBM OpenPages MRG Beta User Guide



Model Risk Management with IBM Watson OpenScale for IBM Cloud Pak for Data & IBM OpenPages MRG

WELCOME to the Model Risk Management closed beta for IBM Watson OpenScale for IBM Cloud Pak for Data and IBM OpenPages Model Risk Governance (MRG). In addition to giving some background information about models, model risk, and how to manage it, this guide takes you through the steps of creating pre-production and production models.

Financial institutions manage many complex and integrated areas of risk. Management of model risk is critical to meet regulatory requirements and to protect institutions from operational and reputational risk. It is precisely this scenario that the closed beta is meant to demonstrate.

What is a Model?

The Federal Reserve and Office of the Comptroller of the Currency guidance SR Letter 11-7 defines a Model as "...a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates."

These types of models, either deterministic or probabilistic, raise different model risk management challenges.

What is Model Risk?

Model risk is a type of risk that occurs when a mathematical model is used in financial institutions to predict and measure quantitative information, and the model performs inadequately. This can lead to adverse outcomes for the firm and operational losses in millions.

Model Development Cycle

There are many challenges with machine learning and deep learning models. For example, you need to face the lack of knowledge of methods used by model developers or vendors, along with inconsistent documentation and increased volume of model change.

Tests to be run on machine learning and deep learning models differ from straightforward application testing:

- Drift: Any change in input data, also known as drift, can cause the model to make inaccurate decisions, impacting business KPIs.
- Bias: Although training data may be cleaned to be free from bias, but runtime data may induce biased behavior of model.
- Explainability: Traditional statistical models are simpler to interpret and explain, but machine and deep learning models can be complex.
- Missing Validation/Test Data: Model training data sets may not capture the range of data or combinations that could be encountered in runtime.

To govern and manage risk, validation and monitoring of AI models are a necessary addition.

OpenScale & OpenPages MRG Integration

IBM offers an end-to-end model risk management solution for financial services with IBM Watson OpenScale and IBM OpenPages with Watson. OpenPages MRG offers model risk governance that enables you to store and manage a comprehensive model inventory. IBM Watson OpenScale monitors and measures outcomes from AI Models across their lifecycle and performs model validations. What is IBM OpenPages Model Risk Governance (MRG)? For more information, see the IBM OpenPages with Watson product page and the IBM OpenPages online help.

Set up your beta environment

Let's get started! Before you begin using the model risk management features, you'll need to set up the following services on IBM Cloud Pak for Data:

- Watson OpenScale, which provides MRM features and metrics
- Watson Machine Learning (2 separate analytic deployment spaces will be created when you run the beta sample notebook, one for pre-production and one for production).
- A database, such as Db2 Warehouse or another Data source available on Cloud Pak for Data
-
- Watson Studio Local, which provides the ability to run notebooks and secure assets, is already deployed on Cloud Pak for Data. You can gain access to this service through the Project area. (The current tutorial demonstrates how to use Watson Studio Local to create the provided sample models, but you can also use any other IDE to build models.)

Integration system credentials (IBM OpenPages MRG)

For your instance of IBM OpenPages, you are provided access to a Docker image that you must download and provision. For information, refer to the OpenPages Beta Installation Guide. After you install OpenPages, you use it to manage models and view the metrics that are generated by Watson OpenScale. Write the information that you need to connect to IBM OpenPages in the following spaces:

URL	
Username	
Password	

Required file

In addition to the previously mentioned services, you must also have the following sample file:

- IBM_CP4DOP_MRM.ipynb

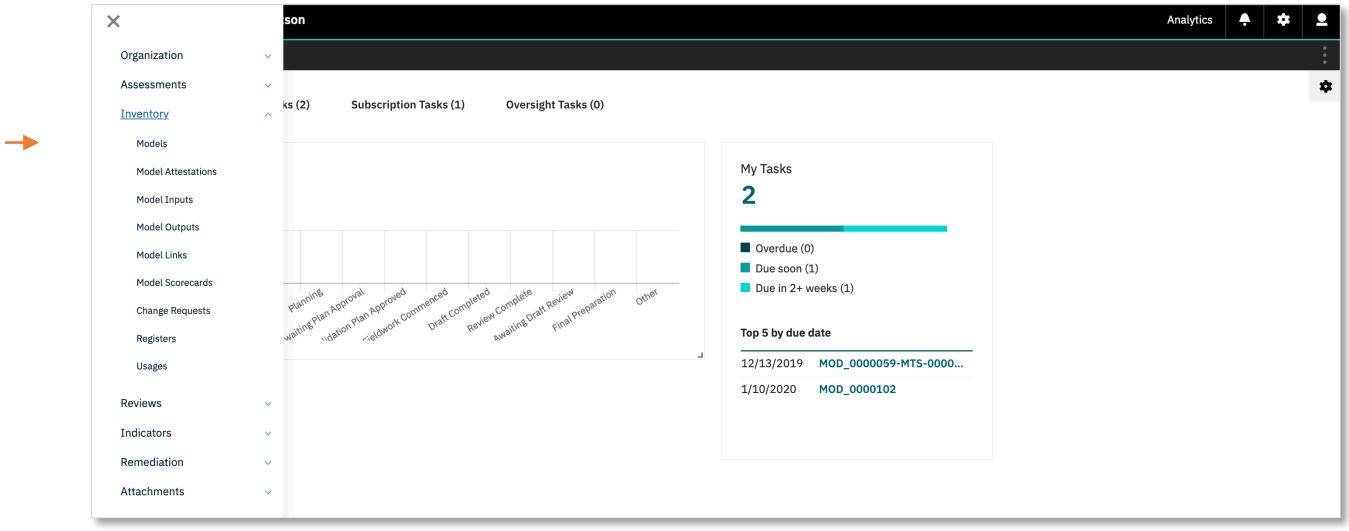
The file can be downloaded from the following Box folder:
https://ibm.box.com/v/modelriskmanagement

Work in IBM OpenPages

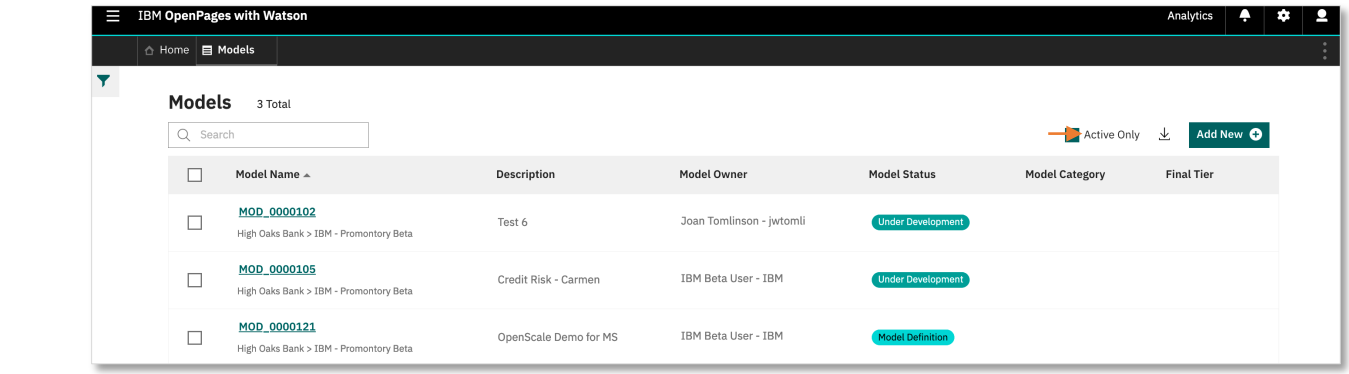
Use this guide to create a new model in OpenPages, take the model through the candidate and development workflows in OpenPages, link the model to an example model OpenScale, explore the OpenScale features, export OpenScale metrics for the model to OpenPages as part of the pre-implementation validation process, and explore the ways to view and interpret these metrics.

Step 1: Set up a New Model in OpenPages

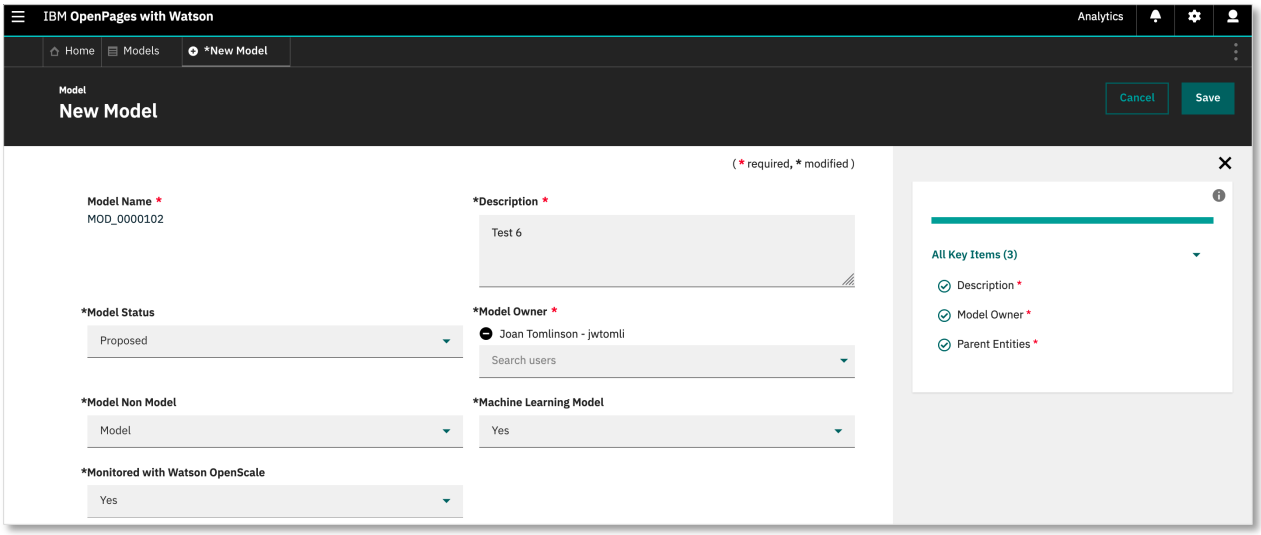
1. Go to menu in the upper left of the screen and select Models under Inventory



2. Click on Add New in the upper right of the screen



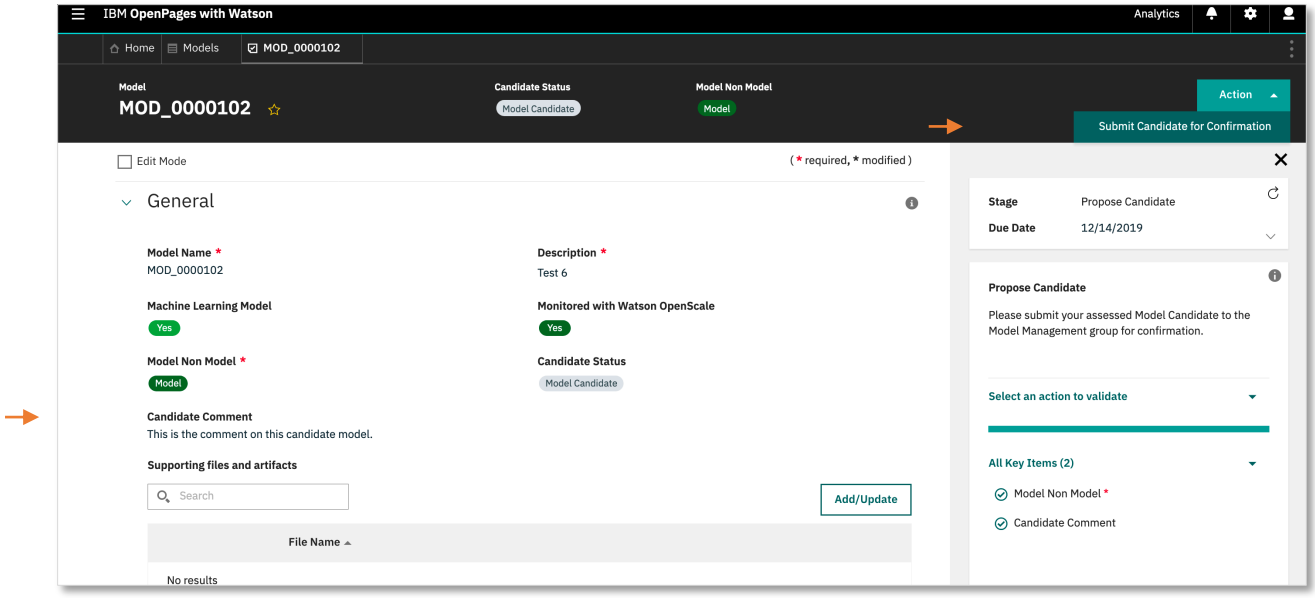
3. Complete the following fields:
    a. Description
    b. Model Status to “Proposed”
    c. Model Owner to your account name
    d. Model Non Model to “Model”
    e. Machine Learning Model to “Yes”
    f. Monitored with OpenScale to “Yes”
        i. This fields appear once Machine Learning Model is set to “Yes”
    g. For Parent Entity select the Business Entity with your organization’s name
4. Click Save



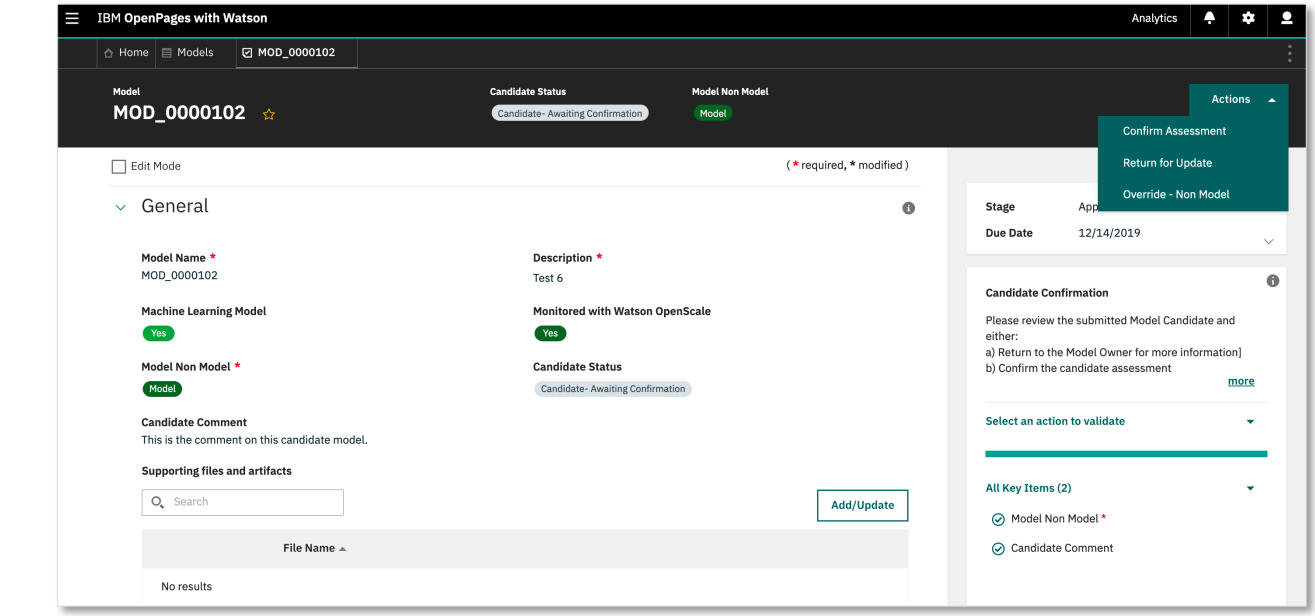
Step 2: Move the Model through the Candidate Workflow

For the closed beta, the typical workflow rules are relaxed to enable the same user to move the model through the workflows. Typically, different stages of the workflow would require users assigned to certain roles such as owner, developer, and head of model review.

1. In the model created in Step 1, enter a Candidate Comment and click Save. This field lets the model owner describe why the proposed model is a model and not a non-model.
2. Select the Action “Submit Candidate for Confirmation.” In a live workflow, this step sends the candidate model to a reviewer for approval.

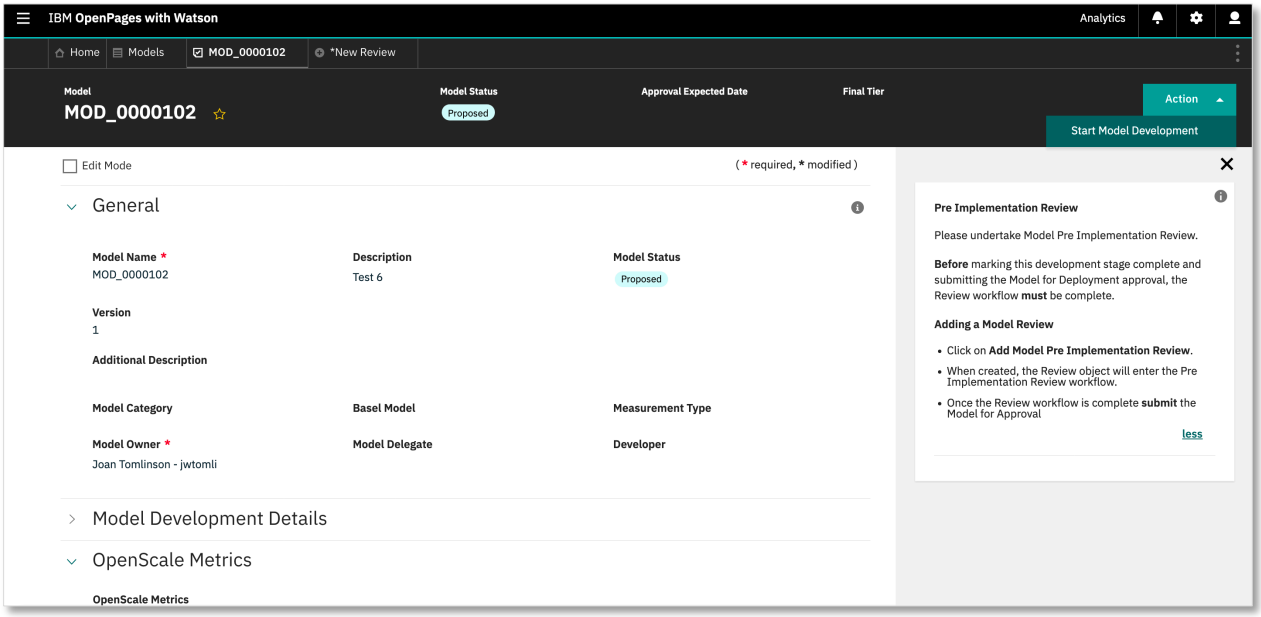


3. Select the Action “Confirm Assessment”. In a live workflow, a reviewer confirms that the model candidate is a model and the candidate workflow is complete.

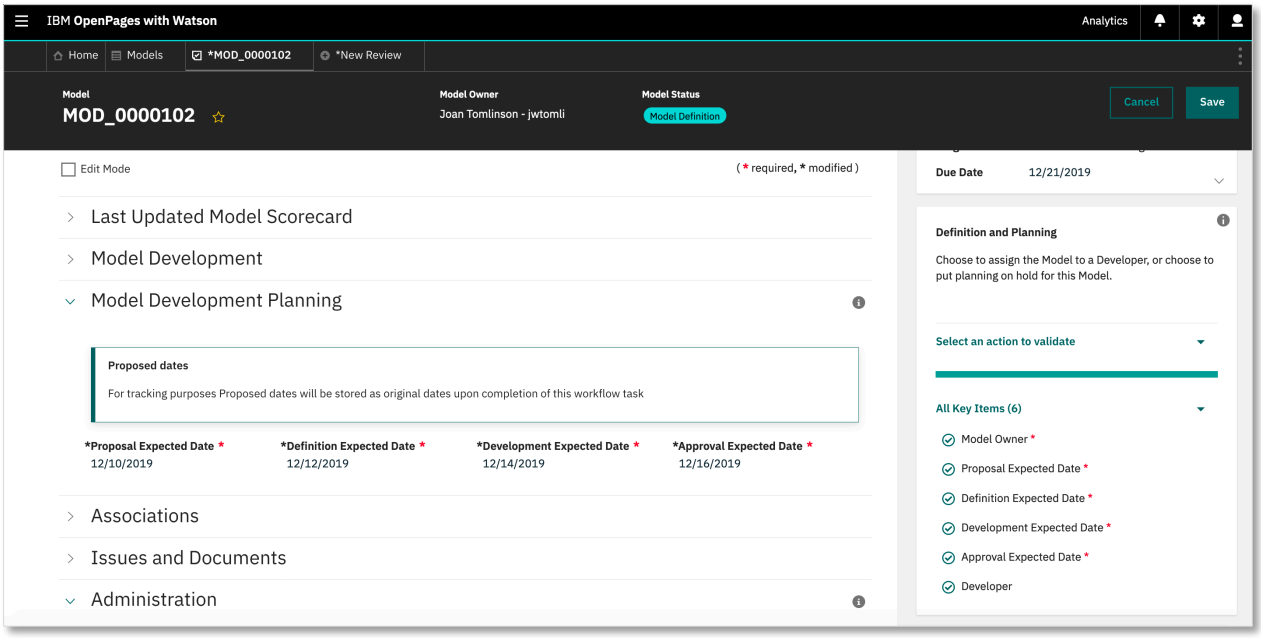


Step 3: Move the Model through the Model Development Workflow to the Pre-Implementation Review Stage

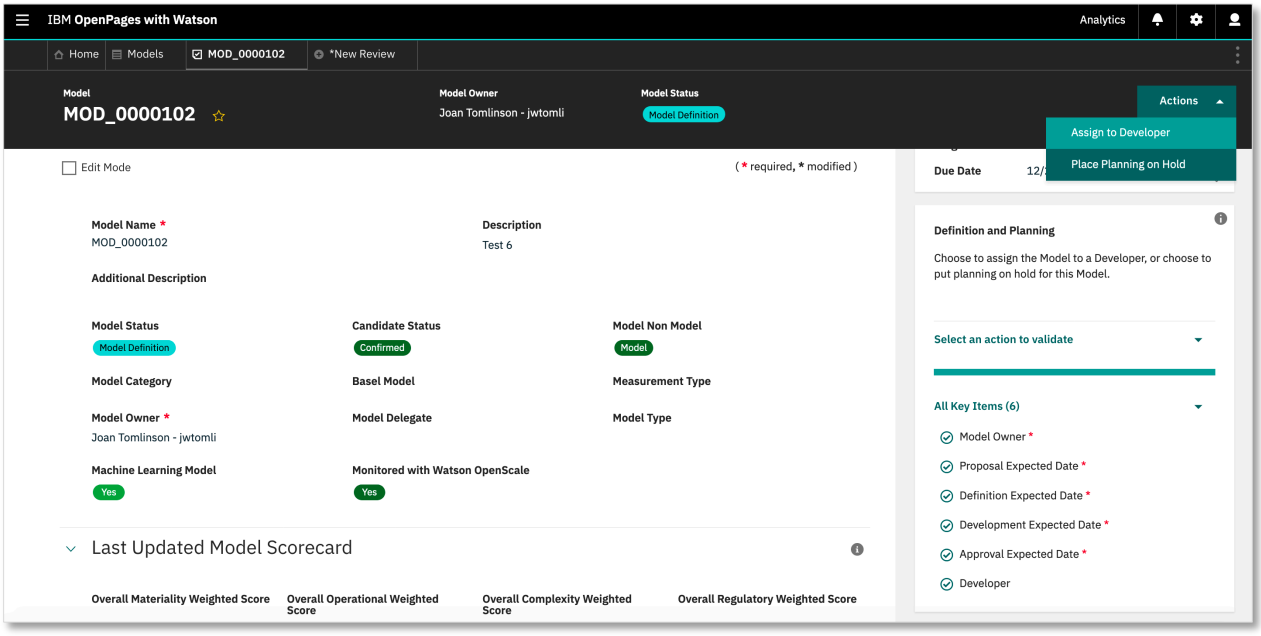
1. From the **Action** drop-down menu, click **Start Model Development**.



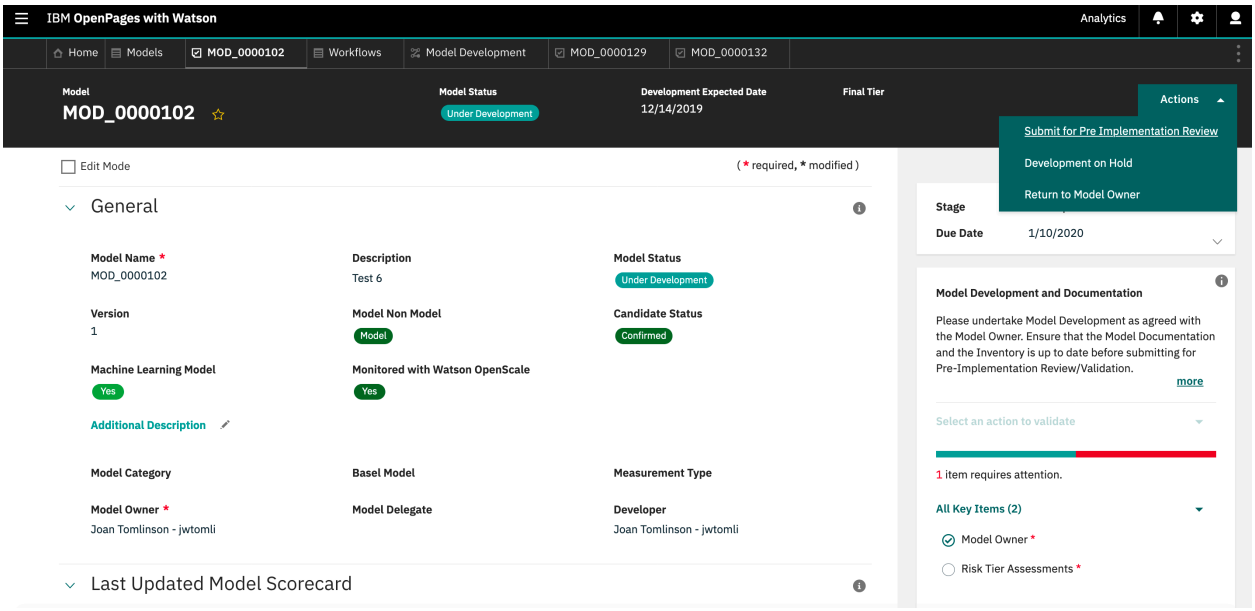
2. Complete the required fields in the Model object that are related to the development – they are listed on the right side panel – and save.
3. For purposes of this testing, you can enter your user account as the developer.



4. Select Action “Assign to Developer”



5. Select Action “Submit for Pre Implementation Review”



Work in Watson Studio Local

In IBM Watson Studio Local, you will create a project and run a notebook to perform most of the set-up tasks, including the following steps:

- create 2 machine models
- connect Watson OpenScale to IBM OpenPages
- create model deployments and configure monitors in Watson OpenScale

Step 1: Create the pre-prod project in Watson Studio

When you first start Watson Studio you have the option of taking a tour. Your first task is to create a project to which you associate the Watson Machine Learning instance that you created for your pre-production work.

1. Click the **Navigation Menu** ( ) icon.
2. Click **Projects**.
3. Click **New Project** and then click the **Create an empty project** tile.
4. Give the project a name and description: In the **Name** field, type **MRM – Pre-prod**. You'll use this project for all your pre-production models.
5. Click the **Create** button.

New project

Step 2: Associate your new project with one of the analytic spaces

Now you need to associate your pre-prod project to an analytic space that you designate for pre-production work. A space is really a category that you can use to control access to your pre-production and production environments. Models are assigned into different spaces, with separate authentication access.

1. From the **MRM – Pre-prod** project window, on the **Overview** tab, click **Associate a new or existing deployment space**.
2. In the **Connect to a deployment space** window, click the **New** tab.
3. Type a name, such as **MRM – pre-prod**, and a description and click the **Associate** button.

Step 3: Add the sample beta notebook to the project

As part of your closed beta information package, you were given access to a Watson Studio notebook. You'll use it to set up your connection between Watson OpenScale and IBM OpenPages, to create and deploy pre-prod models, and configure the model deployments in Watson OpenScale.

1. From the project page, click the **Add to project** button.
2. Click the **Notebook** tile.
3. Click the **From file** tab, click the **Choose file** button and then, select the IBM_CP4DOP_MRM.ipynb notebook file that you can download from https://ibm.box.com/v/modelriskmanagement/
4. Add a name and description and click the **Create notebook** button.

Step 4: Run the sample beta notebook

The newly created notebook is opened in Watson Studio in the integrated notebook editor. You need to update some of the credentials and then run the notebook to create your pre-prod model.

1. In the **Credentials for IBM Cloud Pak for Data** code boxes, paste the following required credentials:
    a. Watson OpenScale credentials (WOS_CREDENTIALS) and GUID (WOS_GUID)
    b. Watson Machine Learning credentials (WML_CREDENTIALS)
    c. Your Db2 credentials (DATABASE_CREDENTIALS)
2. In the **Integration system credentials (IBM OpenPages MRG)** code box, paste the credentials that you received from IBM and copied in the preceding Integration system credentials (IBM OpenPages MRG) section of this Beta Guide.
3. To restart the notebook and clear the output, from the **Kernel** menu, click **Restart & Clear Output**.
4. Run the notebook each cell at a time by using the Run 

option. Ensure that a cell completes before running the next cell. Be sure to read directions for steps that must be taken during the intervening cells. For example, at one point, you are directed to move your model into production before continuing running the notebook.

Congratulations! You have used a notebook to create a pre-prod model. You can check inside Watson Studio, where you will now see the model listed as one of the assets. You have also already deployed this model, which means that you can go to IBM Watson OpenScale to add the model there.

Work in IBM Watson OpenScale

You'll use IBM Watson OpenScale to validate and monitor your models and to process metrics. First, you need to do some set up.

Step 1: Activate model risk management features

As part of the closed beta cohort, you can activate the model risk management beta features on IBM Watson OpenScale. The following sections detail how to activate the beta features on the IBM Cloud Pak for Data environments:

On Cloud Pak for Data

To activate IBM Watson OpenScale in the IBM Cloud Pak for Data environment, you must already have installed IBM Cloud Pak for Data and provisioned your Watson OpenScale instance. Update the environmental variable in the dashboard app by completing the following steps:

1. Open the OpenShift Cluster Console for the **namespace1** name space: https://console.apps.<hostname>-lb-1.fyre.ibm.com/k8s/cluster/namespaces/namespace1
2. Open the **Deployments** page by clicking **Workloads** -> **Deployment**
3. Click **aiopenscale-ibm-aios-dashboard**
4. Click the **Environment** tab and complete the following steps:
    a. Add an environment variable **MRM_ENABLED** by clicking **Add Value** link. (Only for IBM internal builds it is added automatically.)
    b. Change the value of the environment variable **MRM_ENABLED** to **true** (default value is false). When you don't need it, you can delete it by clicking its (-) icon.
5. Click the **Save Changes** button to apply the changes in the pod.

The **aiopenscale-ibm-aios-dashboard** pod is restarted, and the change is applied in the pod.

Note: Ensure that whenever you work inside IBM OpenPages that your profile indicates that you are integrating your work with OpenScale. Also, be sure to select the option **Monitored with Watson OpenScale** when creating your model record.

Step 2: Perform analysis in Watson OpenScale

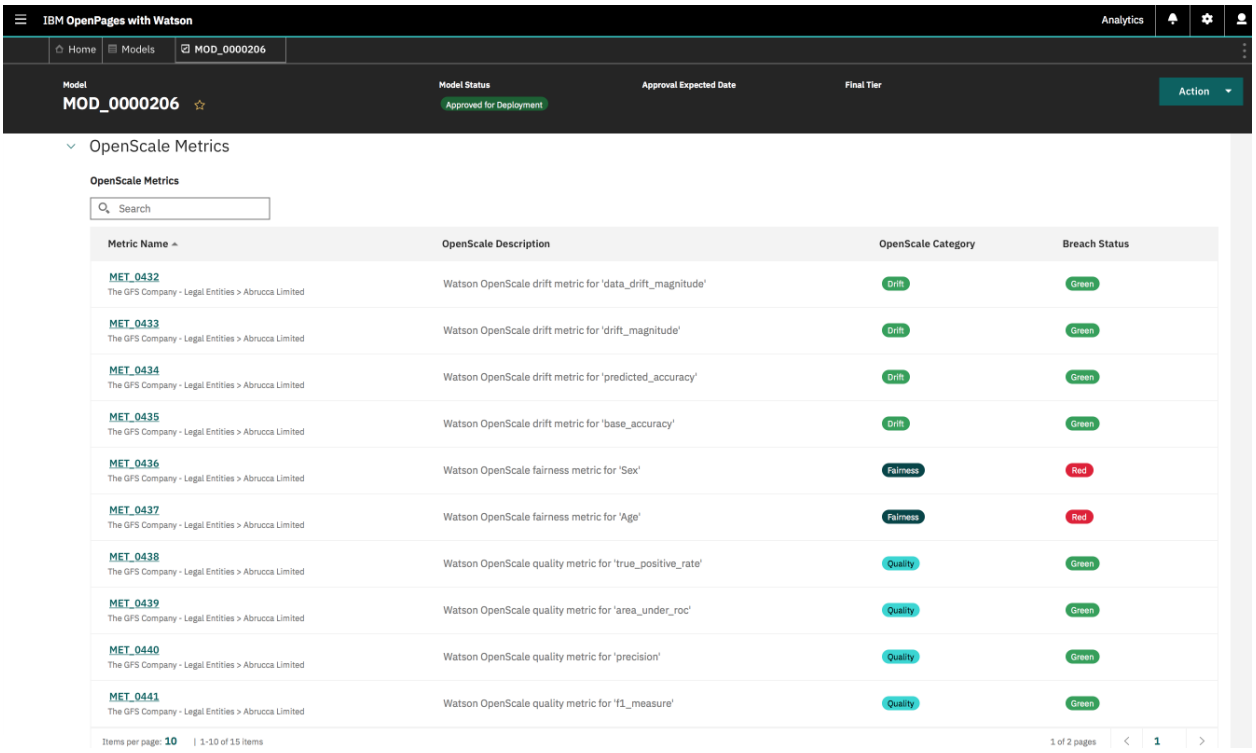
After you run the set-up notebook and activate the MRM beta features, you can both see and compare the sample evaluations in Watson OpenScale. There is a downloadable report, the Model Summary Report, that includes all the quality measures, fairness measures, and drift magnitude.

1. From the **Insights** dashboard, click the model deployment tile
2. From the **Actions** drop-down box, click one of the following analysis options:
    a. **Past evaluations**: Lists all the previous versions of the evaluation.
    b. **Compare**: Compare any of the models, but especially versions of the same model, for best performance.
    c. **Download report PDF**: Generates the model summary report, which gives you all of the metrics and the explanation for why they were scored the way they were.
    d. **Send to OpenPages now**: Sends all the metrics to the OpenPages model record that you associated to the OpenScale model deployment. In OpenPages, the metrics are listed in the graphical flow diagram and are clickable so that you can drill down into each metric.

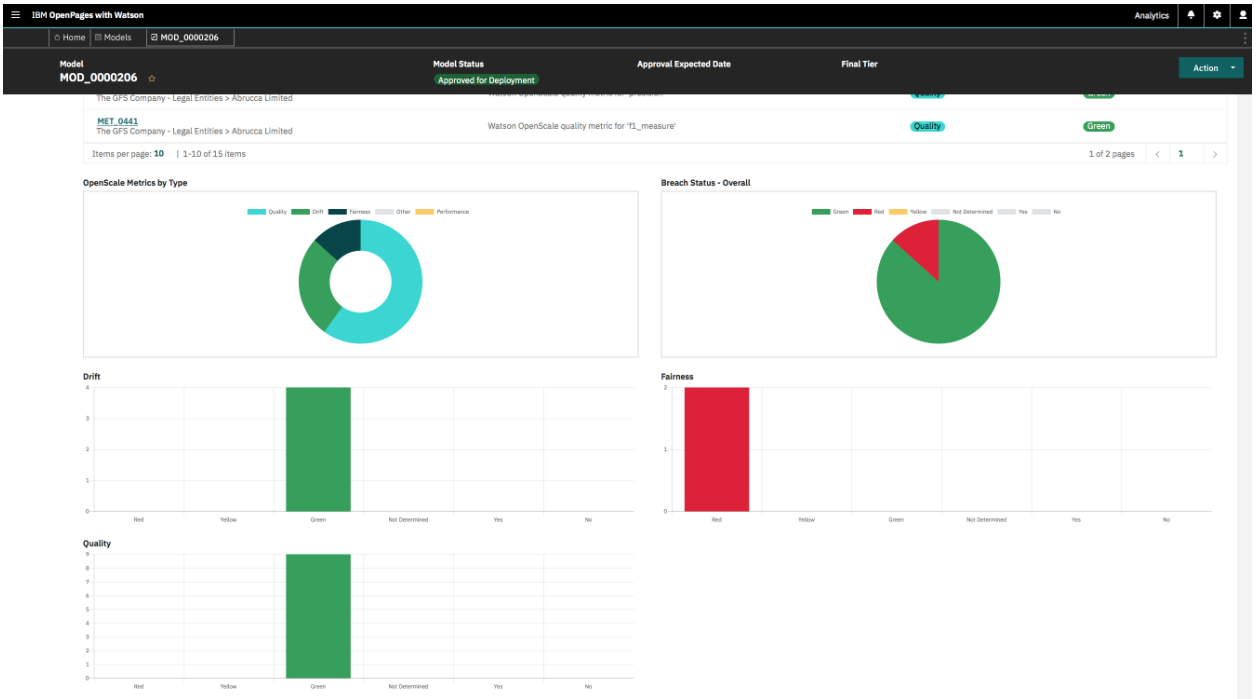
Review results in IBM OpenPages

After you send all the metrics to IBM OpenPages, you are able to review the metrics in OpenPages as part of the Pre-Implementation Review.

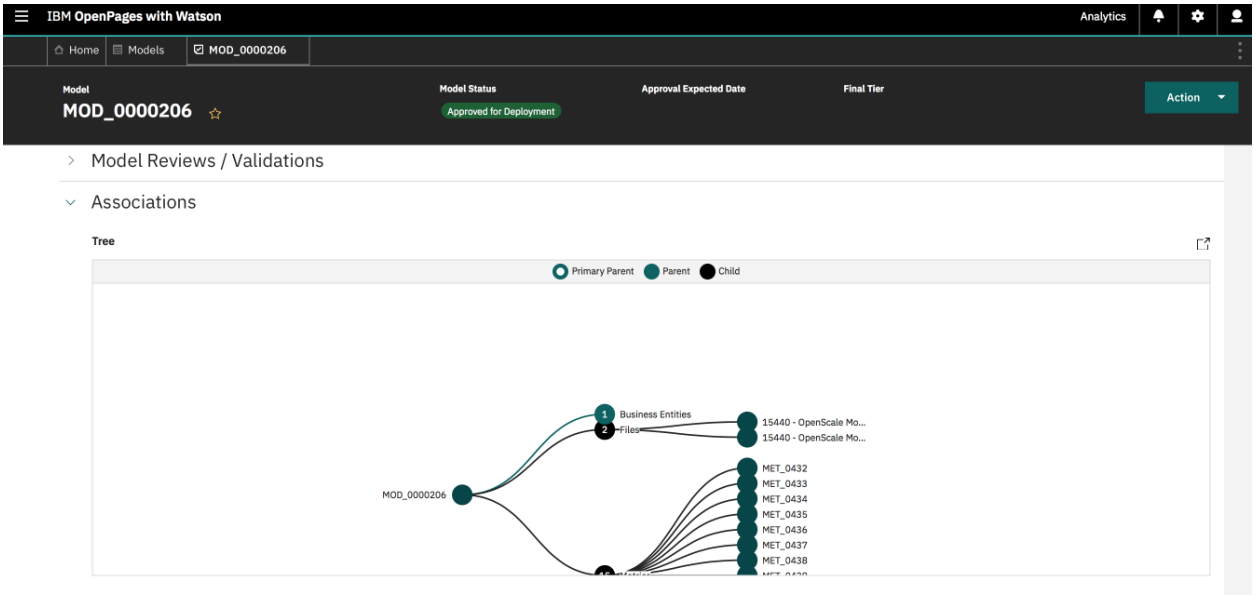
1. Find the model in IBM OpenPages by using the model name, such as MOD_0000206.
2. Review the metrics from Watson OpenScale by expanding the OpenScale Metrics twisty:



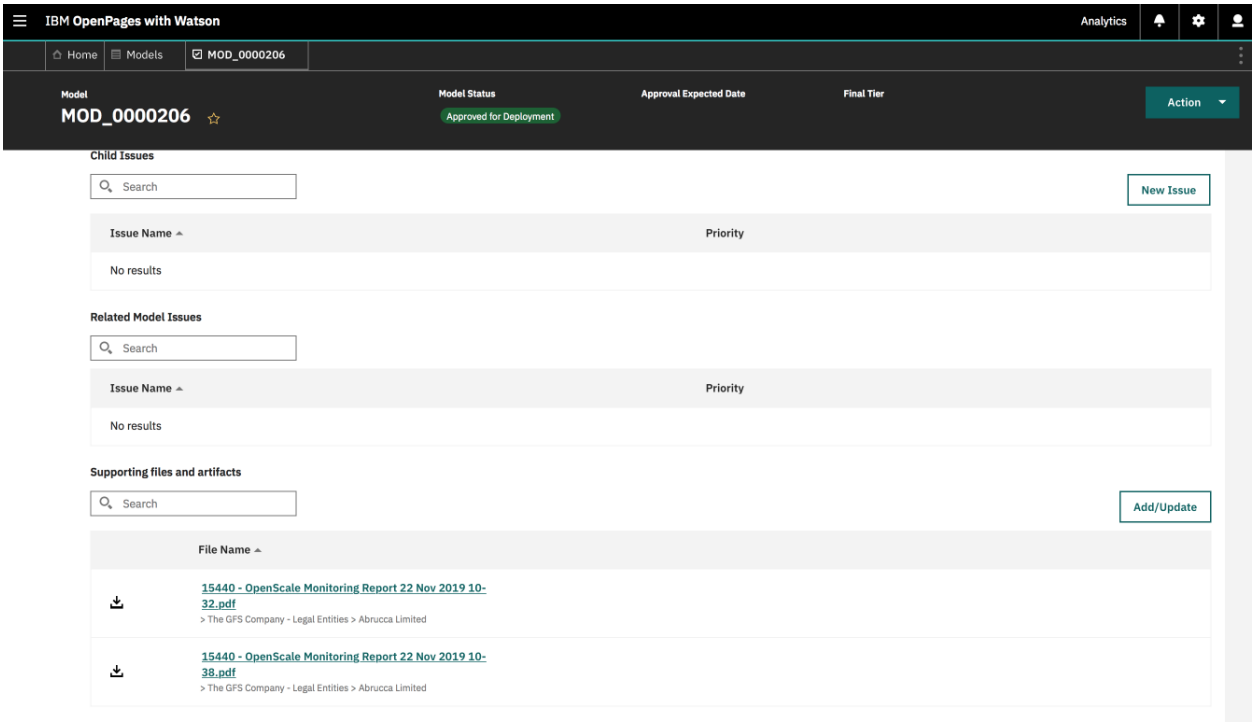
3. In addition to a list of metrics, you can view metrics by type in a graphical format by expanding the OpenScale Metrics Summary twisty:



4. The Associations view provides relationships in the form of a tree:



5. The **Supporting files and artifacts** pane gives you access to all the Watson OpenScale model risk management reports that are run:



Change the model status in IBM OpenPages

As part of the overall model risk governance workflow, the models you create are typically worked on by several different personas or job roles. For example, there might be a data scientist who is the model owner, a model validator, and model reviewer. For the purposes of the beta, you will act in all of these roles to see how the model can progress from one status to the next.

To do this, you must open the model and use the Actions drop-down 

box to set the model status. Use the ID, such as OpenPagesAdministrator that was given to you to be the model owner, validator, and final approver. For the next part of the tutorial, you'll want the status to be Approved for Deployment.

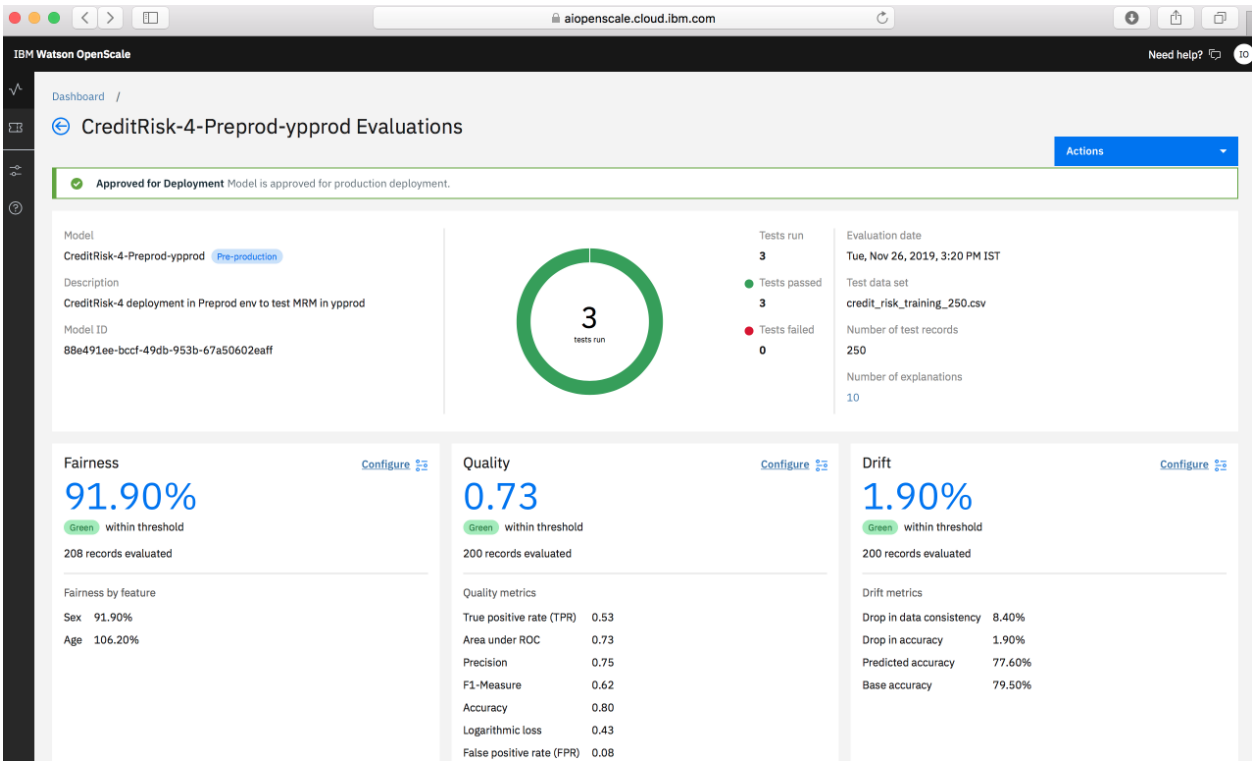
1. In IBM OpenPages, locate the model you want to promote.
2. From the Actions drop-down 

box, click Approved.
If for some reason, you don't see the Approved option, you might need to move the model through other steps, such as **Submit for Pre Implementation Review** or **Submit for Approval**.

Deploy a new model to production in Watson OpenScale

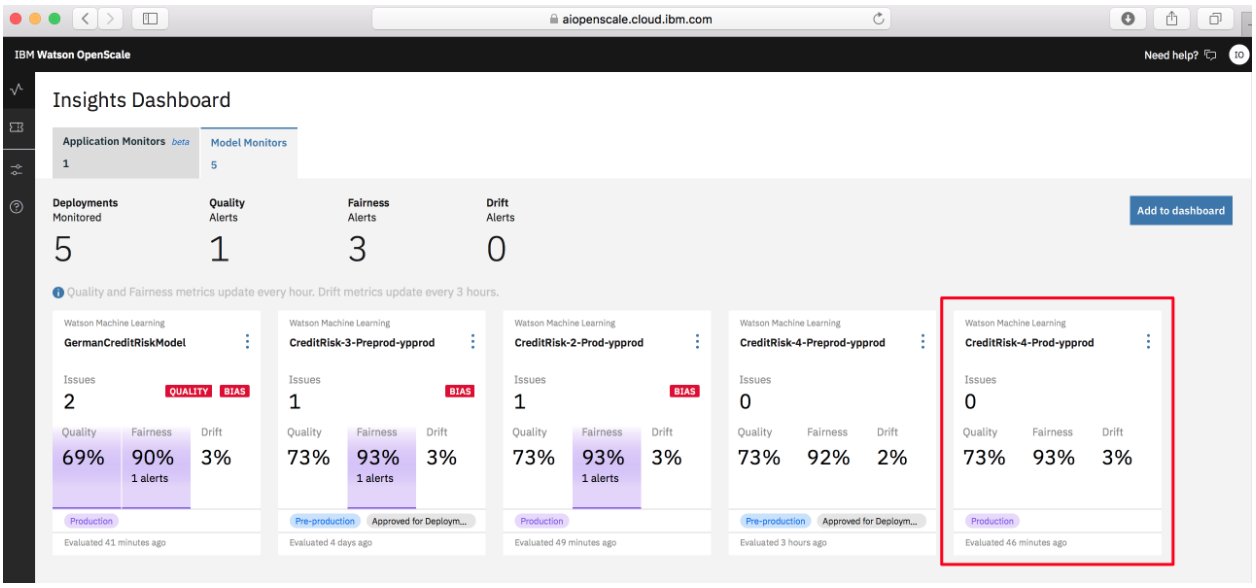
Push the best model to production. Create a production record by importing from a pre-production model. After the model is approved for deployment in IBM OpenPages, you can send the model to production in Watson OpenScale.

1. Review the status of the model deployment:



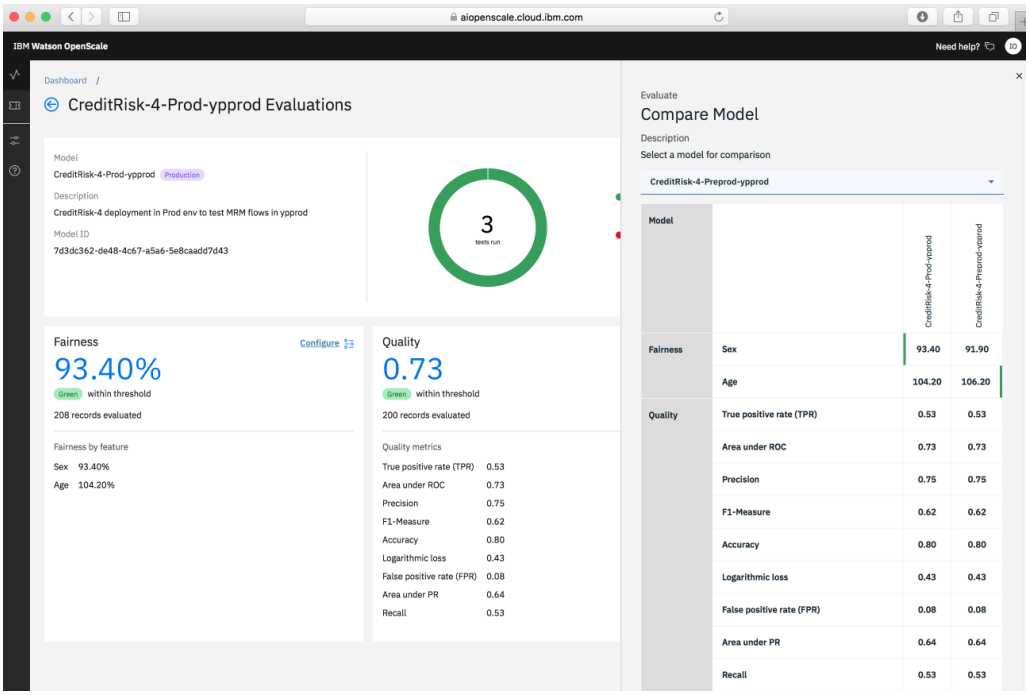
Notebook

2. Return to the **sample beta notebook** and run the cells to send the model to production.
3. You can now view the production model deployment tile. In a regular production environment, it initially appears empty until enough data is gathered and time has passed for metric calculation to be triggered. For the beta, the notebook adds data and runs the monitors so that you can see the results right away.

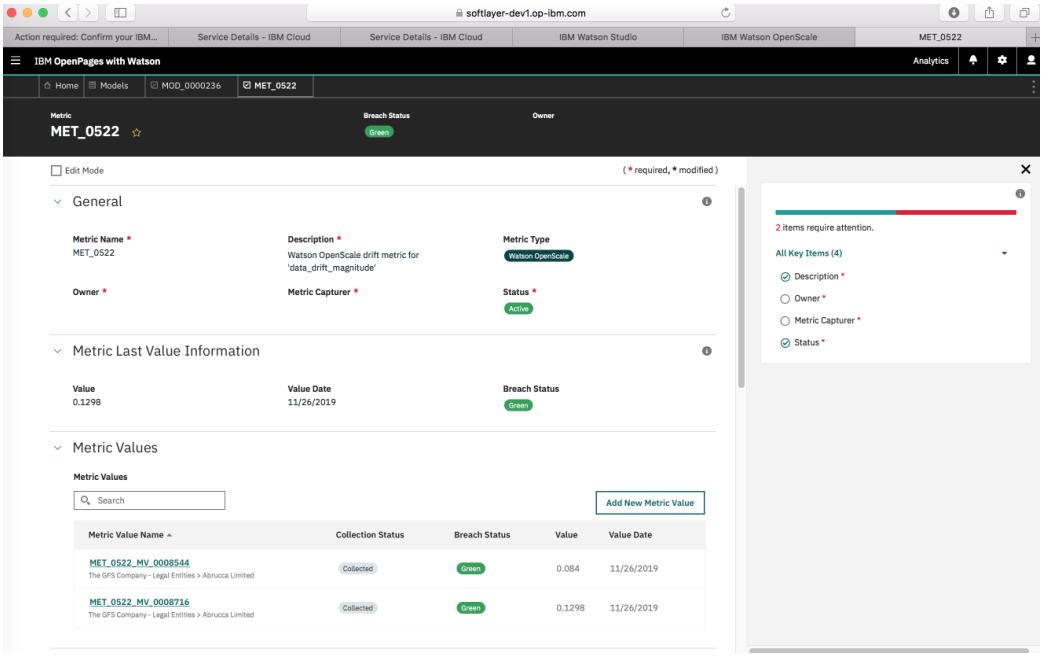


Use the analysis of fairness to redefine the model, possibly by using a different algorithm.

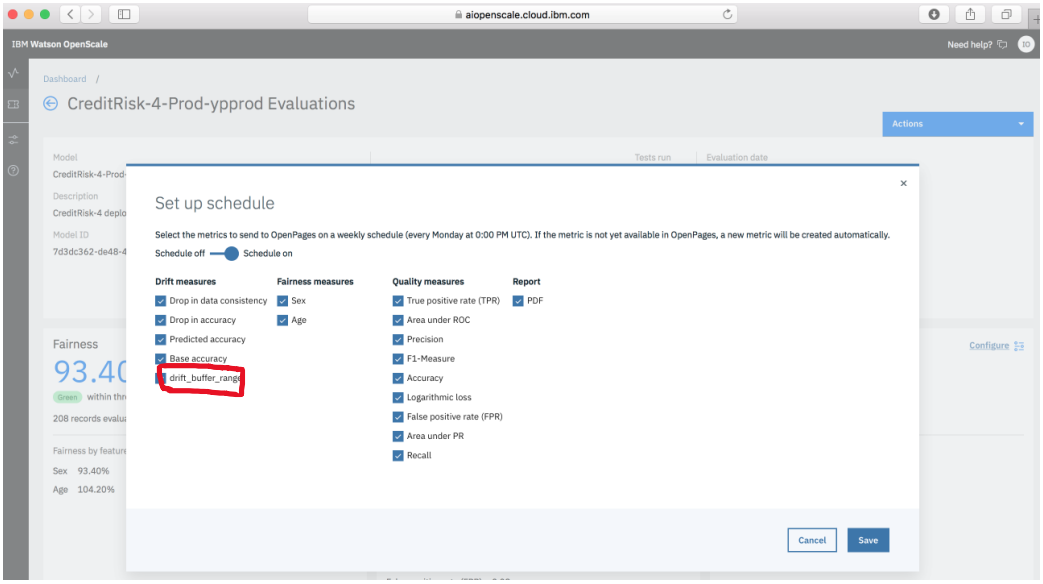
Watson OpenScale enables you to compare models by looking at the key metrics in a side-by-side comparison. Use this feature to determine which version of a model is the best one to send to production or which model might need work:



Because of the connection to Watson OpenScale, you can get alerts in IBM OpenPages for items that require attention or missing pieces of information:



You can set up a regular schedule for sending metrics to IBM OpenPages:



Note: Ensure that the **drift_buffer_range** metric is **de-selected** before saving your schedule. See **Known issues and limitations for beta** for more information.

Known issues and limitations for beta

Because this is a closed beta, you are working in a non-standard and non-production environment. It is expected that there will be some limitations,

issues, and non-standard ways of working. At the start of the closed beta, the offering management team is aware of the following issues:

Publishing metrics from Watson OpenScale to IBM OpenPages MRG fails on Cloud Pak for Data

If you selected all (or specifically the **drift_buffer_range** metric) metrics while publishing metrics to OpenPages, it fails with the following error: "message_details": "float() argument must be a string or a number, not 'list'"

Because publishing metrics to IBM OpenPages happens as a single metric at a time, some metrics are published until the processor encounters the **drift_buffer_range** metric, which causes it to subsequently fail.

Ensure that you de-select the **drift_buffer_range** metric before sending metrics to IBM OpenPages.

Common log per client for IBM OpenPages

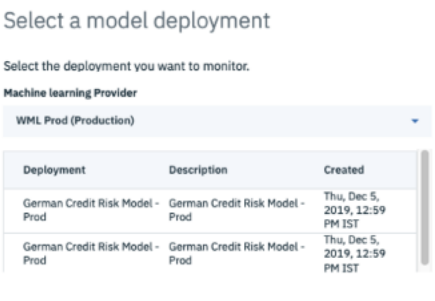
Because each client in the closed beta is assigned a single user ID for IBM OpenPages, there will be a single common log that is available to every participant in the closed beta. Clients are responsible for ensuring that no proprietary or personally identifiable information is recorded in the IBM OpenPages log.

Payload logging requires additional submissions for Amazon Web Services binary, Microsoft Azure binary and multiclass, and Native XGBoost binary problem types

If you build your own notebook to try out model risk management features for any of the models that use certain frameworks, you must send the same record for initial scoring a second time. This is needed for the initial setup of payload logging when you configure monitors. The following frameworks and problem types are affected:

- Amazon Web Services binary
- Microsoft Azure binary and multiclass
- Native XGBoost binary

Duplicate deployments appear in the list of deployments when you add a production model to the Insights dashboard



When you attempt to add a production model to the Insights dashboard, you actually see two listings for the same model.

These are identical and you can choose either item to add to the dashboard.