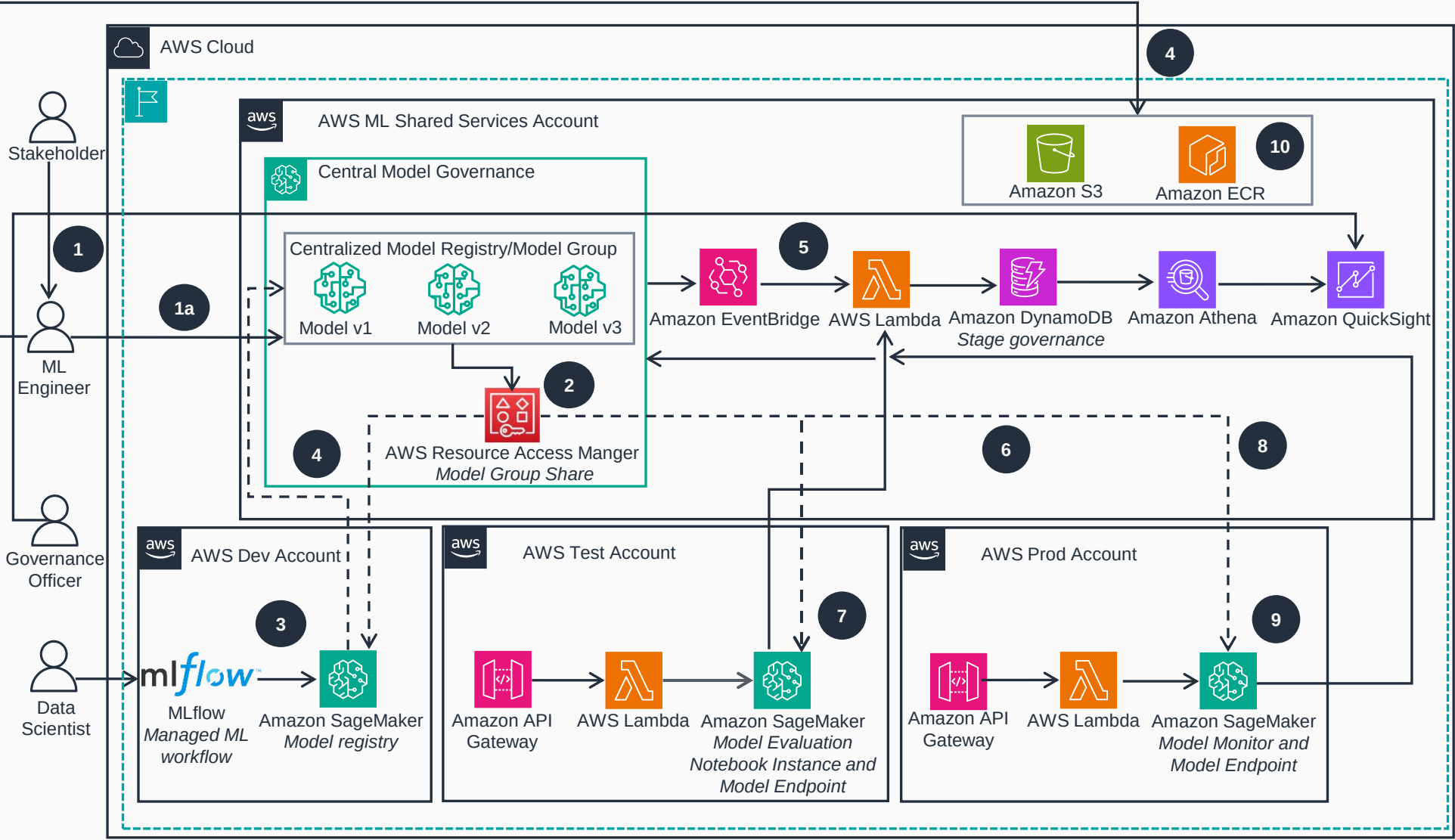


Guidance for Multi-Account Machine Learning Model Governance on AWS

This architecture diagram shows a centralized model governance approach using AWS Resource Access Manager (AWS RAM). With AWS RAM, you can share models using the Amazon SageMaker Model Package Group, a fundamental construct within the Amazon SageMaker Model Registry where Model Package Versions are registered. Steps 1-4 out of 10 are shown here; steps 5-10 are shown on the next slide.



1 The stakeholder, specifically the Data Scientist (DS) team lead, receives a request from the business leader to develop an AI use case, such as a credit risk model.

1a. The Machine Learning Engineer (MLE) is notified to establish a model group for the development of a new model. The MLE then creates the necessary infrastructure pipeline to set up the new model package group.

2 The MLE sets up the pipeline to share the model group with the necessary permissions (create, describe, update model version) to the ML project team's development account. Optionally, the package group can also be shared with the test and production accounts if local account access to model versions is required.

3 The DS uses MLflow, an open-source platform for managing the end-to-end machine learning lifecycle. MLflow is used within **Amazon SageMaker Studio** to construct model experiments, select a candidate model, and register the model version within the shared model group in the local **Amazon SageMaker Model Registry**.

4 Since this is a shared model group, the model version metadata will be recorded in the Centralized Model Registry, and a corresponding link will be maintained in the development account. The MLE can set up **Amazon Simple Storage Service** (Amazon S3) and **Amazon Elastic Container Registry** (Amazon ECR) in the shared account, allowing the DS to store the model artifacts from the development account. The DS is granted the necessary permissions to access the model artifacts in **Amazon S3** and **Amazon ECR** within the shared services account.



Guidance for Multi-Account Machine Learning Model Governance on AWS

Steps 5-10

