

IBM watsonx.governance for machine learning models

Accelerate responsible, transparent
and explainable AI workflows



Highlights

Automate AI governance
across the machine
learning model lifecycle

Proactively detect and
mitigate risks according
to priority

Improve compliance
policies, industry standards
and AI regulations

Machine learning (ML) models use predictive analytics to identify trends and patterns in data, learning from their experience to make more accurate analytics decisions. Use cases for ML include medical image analysis and diagnosis, speech recognition, natural language processing (NLP), text classification, sentiment analysis and fraud detection. Unfortunately, the process of ensuring the accuracy and fairness of these models is often hindered by the absence of an automated platform with tools and processes optimized for AI, lack of transparency and explainable results, and inadequate stakeholder communication and collaboration tools.

IBM watsonx.governance automates model processes across the AI lifecycle. It provides enterprise-level rigor and human oversight into how models are created and deployed both on premises and in the cloud, helping organizations meet growing ML model challenges. It uses one unified, integrated platform for governing ML and generative AI.



Comprehensive. Provides governance for both ML and generative AI in one hybrid, integrated platform



End to end. Includes lifecycle governance and risk management to support compliance with internal policies, industry standards and AI regulations

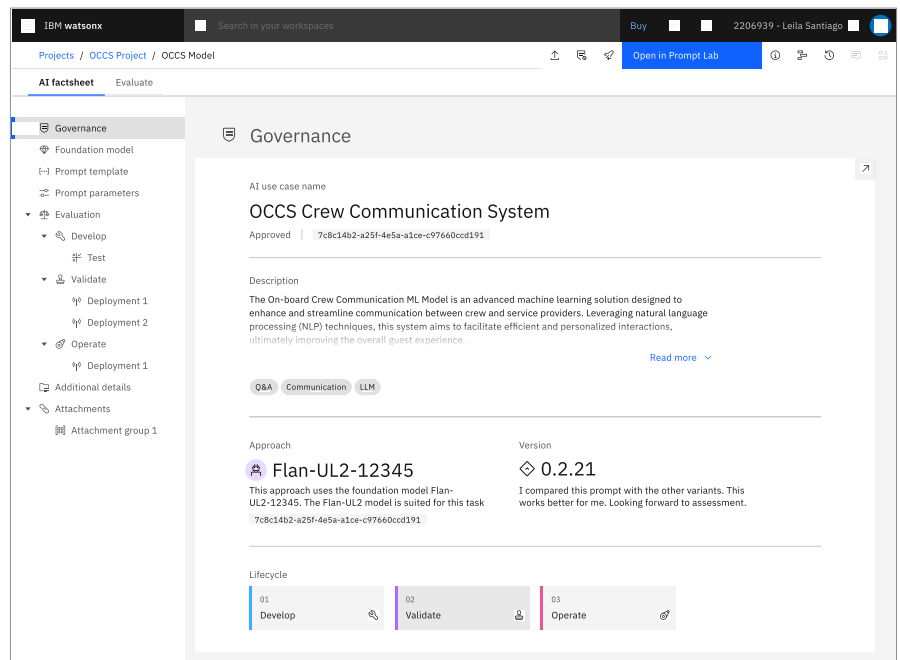


Open. Supports third-party tools (e.g., AWS, Microsoft and Google) for ML models currently in place—no need to rip and replace

Automate AI governance across the ML model lifecycle

Lifecycle governance: Accelerate model building at scale. Automate and consolidate multiple tools, applications and platforms while documenting the origin of datasets, models, associated metadata and pipelines.

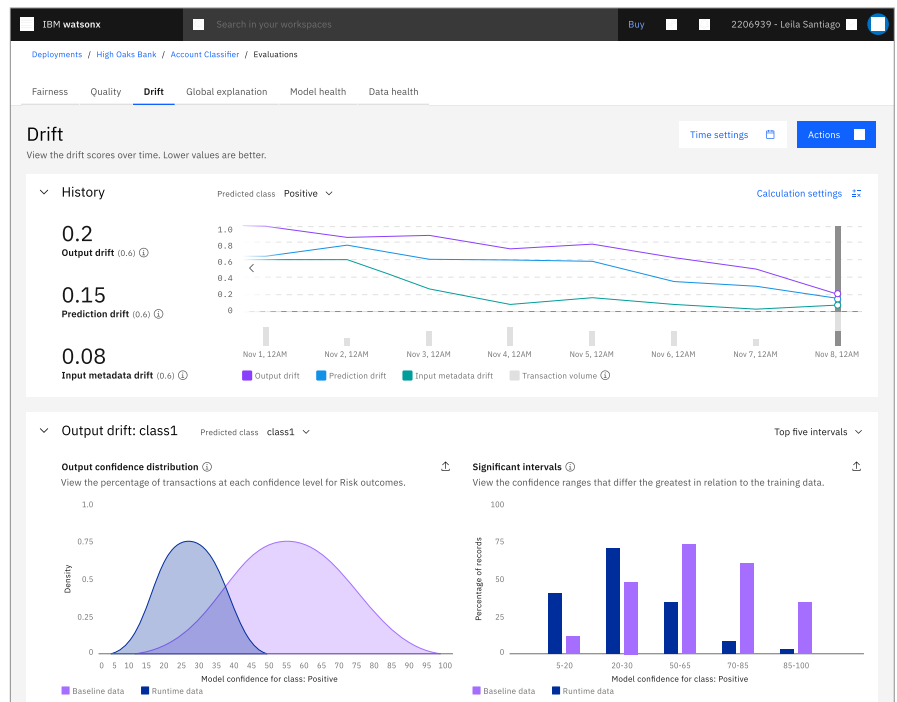
- Monitor, catalog and govern models across the AI lifecycle from anywhere. Free up time and automate workflows to build and deploy models at scale.
- Capture model metadata for effortless report generation.
- Use the Factsheets feature to allow model validators and approvers access to an accurate, real-time view of model lifecycle details.
- Increase accuracy of predictions by proactively identifying bias, drift and retraining opportunities.
- Improve stakeholder communications and collaboration with tools and customizable dashboards.



Proactively detect and mitigate risks according to priority

Enable responsible, explainable, high-quality AI models and automate documentation of model lineage and metadata. Monitor for fairness, bias and drift and set alert tolerances for timely risk mitigation.

- Access an automated, scalable, AI governance risk and compliance (GRC) toolkit.
- Drive fair decisions with the ability to adjust to changes in behavioral patterns and profiles with model retraining or rebuilding.
- Use the Factsheets capability, fact capture and documentation automation for model validators and approvers to access an accurate, real-time view that provides explainability of model results.
- Increase stakeholder visibility with dynamic, user-based dashboards, charts and dimensional reporting. Provide explainable results with an enterprise-wide view of risk for all business units, partners and suppliers.



Improve compliance policies, industry standards and AI regulations
 Support regulatory compliance using protections and validation to build and deploy models that are fair, transparent and compliant. Automatically document model facts in support of audits.

- Translate external AI regulations into global policies for automated enforcement.
- Enhance compliance for audit and reporting purposes through Factsheets documentation.
- Access an automated and scalable GRC platform that helps to effectively manage IT and security risks, reduce costs and meet compliance requirements.
- Connect internal GRC policies and practices to the external regulatory environment.



AI use case					
Name	Insurance claims processing				
ID	35086564-c181-44a1-8f9b-231302acfa25				
Status	Developed Dimitri Hoffmann (DHOFF@du.ibm.com) Nov 12 2023, 12:32 PM GMT				
Description	This is a demo use case where we would like to automatically process claims from our customers about their car insurance cases. With the help of AI we would like to automate summarization of customer written claims in a standardized way. Additionally, we want to make use of AI to provide next steps for our internal support teams.				
Risk level	medium				
Tags	ETA Prompt engineering GenAI				
Created by	Dimitri Hoffmann (DHOFF@du.ibm.com)				
Created	Nov 08 2023, 13:54 PM GMT				
Last modified	Nov 16 2023, 13:39 PM GMT				
Approaches used in this AI use case <table border="1"> <thead> <tr> <th>Approach name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Prompt Engineering (flan-t5-xl)</td> <td>This approach tackles the use case with prompt engineering of the flan-t5-xl foundation model.</td> </tr> </tbody> </table>		Approach name	Description	Prompt Engineering (flan-t5-xl)	This approach tackles the use case with prompt engineering of the flan-t5-xl foundation model.
Approach name	Description				
Prompt Engineering (flan-t5-xl)	This approach tackles the use case with prompt engineering of the flan-t5-xl foundation model.				
Additional AI use case details Risk level: Model purposes: Supporting documentation:					
AI asset instance tracking This AI use case tracks 2 AI asset versions: "Insurance claims suggested next steps" with instances in 3 environments of (spati) Production "Insurance claims summarization" with instances in 3 environments of (spati) Development, Pre production, Production					



Conclusion

IBM watsonx.governance accelerates responsible, transparent and explainable AI using automated tools and processes built to direct, manage and monitor models across the AI lifecycle. It lets you proactively detect and mitigate risks and better meet compliance requirements, including internal policies, industry standards and the changing regulatory landscape. IBM watsonx.governance provides governance for both traditional ML and generative AI models on an open, integrated platform. Deploy the solution both on premises and in the cloud.

Why IBM?

IBM watsonx is our next-generation, enterprise AI and data platform. It includes IBM watsonx.data, IBM watsonx.ai and IBM watsonx.governance—all of which are designed to help scale and accelerate the impact of AI across your business. IBM watsonx is trusted to manage the most business-critical applications across cloud and on-premises deployments.

For more information

To learn more about watsonx.governance, contact your IBM representative or IBM Business Partner or visit ibm.com/products/watsonx-governance.

© Copyright IBM Corporation 2023

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
November 2023

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation, in the U.S. and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Generally expected results cannot be provided as each client's results will depend entirely on the client's systems and services ordered. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products, or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

