

# IBM watsonx.governance für Modelle für maschinelles Lernen

Beschleunigen Sie verantwortungsvolle,  
transparente und erklärbare KI-Workflows

## Wesentliche Vorteile

Automatisierung der  
KI-Governance über den  
gesamten Lebenszyklus von  
Modellen für maschinelles  
Lernen hinweg

Proaktive Erkennung und  
Minderung von Risiken je  
nach Priorität

Verbesserung der  
Compliance- Richtlinien,  
Branchenstandards  
und KI-Vorschriften

Modelle des maschinellen Lernens (ML) nutzen prädiktive Analysen, um Trends und Muster in Daten zu erkennen und aus ihren Erfahrungen zu lernen, um präzisere analytische Entscheidungen zu treffen. Zu den Anwendungsfällen für ML gehören medizinische Bildanalyse und -diagnose, Spracherkennung, Verarbeitung natürlicher Sprache (NLP), Textklassifizierung, Stimmungsanalyse und Betrugserkennung. Leider wird der Prozess zur Sicherstellung der Genauigkeit und Fairness dieser Modelle oft behindert – durch das Fehlen einer automatisierten Plattform mit für KI optimierten Tools und Prozessen, durch mangelnde Transparenz und erklärbare Ergebnisse sowie durch unzureichende Tools für die Kommunikation und Zusammenarbeit mit den Stakeholdern.

IBM watsonx.governance automatisiert Modellprozesse über den gesamten KI-Lebenszyklus hinweg. So werden die Erstellung und der Einsatz von Modellen sowohl vor Ort als auch in der Cloud auf Unternehmensebene streng überwacht, was Unternehmen dabei unterstützt, die wachsenden Anforderungen an ML-Modelle zu erfüllen. IBM watsonx.governance verwendet eine einheitliche, integrierte Plattform für die Steuerung von ML und generativer KI.



**Umfassend.** Bietet Governance sowohl für ML als auch für generative KI in einer hybriden, integrierten Plattform



**End-to-End.** Beinhaltet Lebenszyklus-Governance und Risikomanagement zur Unterstützung der Compliance mit internen Richtlinien, Branchenstandards und KI-Vorschriften



**Offen.** Unterstützt Tools von Drittanbietern (z. B. AWS, Microsoft und Google) für ML-Modelle, die bereits im Einsatz sind – es ist nicht nötig, sie zu entfernen und zu ersetzen

## Automatisierung der KI-Governance über den gesamten Lebenszyklus von ML-Modellen

**Lebenszyklus-Governance:** Beschleunigen Sie die Modellerstellung im großen Maßstab. Automatisieren und konsolidieren Sie mehrere Tools, Anwendungen und Plattformen, während Sie den Ursprung von Data Sets, Modellen, zugeordneten Metadaten und Pipelines dokumentieren.

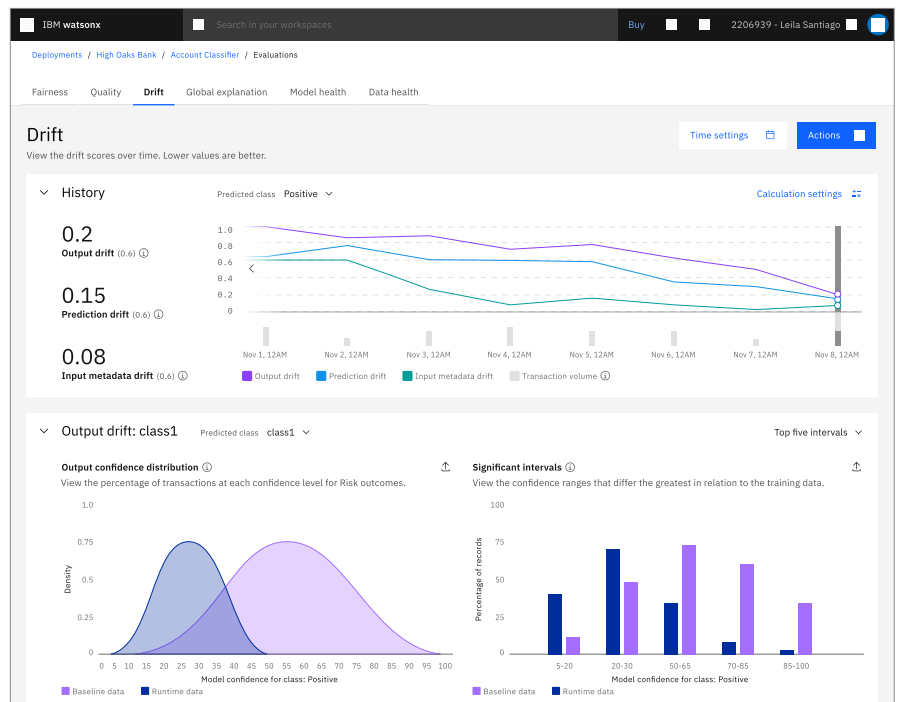
- Überwachen, katalogisieren und steuern Sie Modelle standortunabhängig im gesamten KI-Lebenszyklus. Verschaffen Sie sich Zeit und automatisieren Sie Workflows, um Modelle in großem Maßstab zu erstellen und bereitzustellen.
- Erfassen Sie Modellmetadaten für eine mühelose Berichterstellung.
- Verwenden Sie die Funktion Factsheets, um Modellvalidatoren und -Genehmigern Zugang zu einer präzisen Echtzeitsicht der Details des Modelllebenszyklus zu ermöglichen.
- Erhöhen Sie die Prognosegenauigkeit durch proaktives Erkennen von Bias, Drift und Umschulungsmöglichkeiten.
- Verbessern Sie die Kommunikation und Zusammenarbeit mit Ihren Stakeholdern durch Tools und anpassbare Dashboards.

The screenshot displays the IBM Watsonx Governance interface. The top navigation bar includes 'IBM watsonx', a search bar, and user information 'Buy 2206939 - Lelia Santiago'. The main content area is titled 'Governance' and shows details for the 'OCCS Crew Communication System' model. The interface is divided into a left sidebar with navigation options like 'Foundation model', 'Prompt template', 'Evaluation', 'Develop', 'Test', 'Validate', 'Deployment', 'Operate', 'Additional details', and 'Attachments'. The main panel displays the model's name, approval status, description, approach (Flan-UL2-12345), version (0.2.21), and a lifecycle progress bar with stages: 01 Develop, 02 Validate, and 03 Operate.

## Proaktive Erkennung und Abschwächung von Risiken je nach Priorität

Ermöglichen Sie verantwortungsvolle, erklärbare, qualitativ hochwertige KI-Modelle und automatisieren Sie die Dokumentation der Modellherkunft und der Metadaten. Überwachen Sie Fairness, Bias und Drift und legen Sie Alarmtoleranzen fest, um frühzeitig Risiken zu minimieren.

- Greifen Sie auf ein automatisiertes, skalierbares KI-Toolkit für Governance, Risiko und Compliance (GRC) zu.
- Sorgen Sie für faire Entscheidungen mit der Fähigkeit, sich an veränderte Verhaltensmuster und -profile anzupassen, indem Sie das Modell neu trainieren oder neu aufbauen.
- Nutzen Sie die Funktionen Factsheets, Faktenerfassung und Dokumentationsautomatisierung für Modellvalidatoren und -Genehmigern, um auf eine genaue Echtzeit-Ansicht zuzugreifen, die Ihnen erklärbare Modellergebnisse bereitstellt.
- Verbessern Sie die Sichtbarkeit für Ihre Stakeholder mit dynamischen, benutzerbasierten Dashboards, Diagrammen und dimensionaler Berichterstattung. Liefere erklärbare Ergebnisse mit einer unternehmensweiten Sicht der Risiken für alle Geschäftsbereiche, Partner und Lieferanten.



## Verbesserung der Compliance-Richtlinien, Branchenstandards und KI-Vorschriften

Unterstützen Sie die Compliance mit gesetzlichen Vorschriften durch Schutzmaßnahmen und Validierung, um Modelle zu erstellen und einzusetzen, die fair, transparent und konform sind. Dokumentieren Sie automatisch Modellfakten zur Unterstützung von Audits.

- Umsetzung externer KI-Vorschriften in globale Richtlinien zur automatischen Durchsetzung.
- Verbessern Sie die Compliance für Audit- und Berichtszwecke durch die Dokumentation mit Factsheets.
- Greifen Sie auf eine automatisierte und skalierbare GRC-Plattform zu, die Sie dabei unterstützt, IT- und Sicherheitsrisiken effektiv zu verwalten, Kosten zu senken und Compliance-Anforderungen zu erfüllen.
- Verbinden Sie interne GRC-Richtlinien und -Praktiken mit dem externen regulatorischen Umfeld.



AI use case	
Name	Insurance claims processing
ID	3508654-4-e381-44a1-84f9-231102acta25
Status	Developer   Dimitri Hoffmann [DHOFF@de.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) (Demo)
Created by	Dimitri Hoffmann [DHOFF@de.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	
Approach name	Description
Prompt Engineering (Ran-UK2)	This approach backs the use case with prompt engineering of the Ran-UK2 foundation model.
Additional AI use case details	
Risk level: Model purpose: Supporting documentation:	
AI asset instance tracking	
This AI use case tracks 2 AI asset version(s). 1. "Insurance claim suggested next steps" with instances in 3 environment(s) of Special Production 2. "Insurance claim summarization" with instances in 3 environment(s) of Special Development, Pre-production, Production	



### **Zusammenfassung**

IBM watsonx.governance beschleunigt verantwortungsvolle, transparente und erklärbare KI mit automatisierten Tools und Prozessen, die für die Steuerung, Verwaltung und Überwachung von Modellen über den gesamten KI-Lebenszyklus hinweg entwickelt wurden. Damit können Sie proaktiv Risiken erkennen und mindern und Compliance-Anforderungen besser erfüllen, einschließlich interner Richtlinien, Branchenstandards und der sich verändernden regulatorischen Landschaft. IBM watsonx.governance bietet Governance sowohl für traditionelle ML-Modelle als auch für generative KI-Modelle auf einer offenen, integrierten Plattform. Stellen Sie die Lösung sowohl On-Premises als auch in der Cloud bereit.

### **Gründe für IBM?**

IBM watsonx ist unsere unternehmenstaugliche KI- und Datenplattform der neuesten Generation. Sie umfasst IBM watsonx.data, IBM watsonx.ai und IBM watsonx.governance – allesamt dafür konzipiert, die Auswirkungen von KI auf Ihr Unternehmen zu skalieren und zu beschleunigen. IBM watsonx verwaltet zuverlässig die geschäftskritischsten Anwendungen in der Cloud und On-Premises.

### **Weitere Informationen**

Wenn Sie mehr über watsonx.governance erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM or IBM Business Partner oder besuchen Sie [ibm.com/de-de/products/watsonx-governance](https://ibm.com/de-de/products/watsonx-governance).

© Copyright IBM Corporation 2023

IBM Deutschland GmbH  
IBM-Allee 1  
71139 Ehningen  
[ibm.com/de](http://ibm.com/de)  
IBM Corporation  
New Orchard Road  
Armonk, NY 10504

Hergestellt in den  
Vereinigten Staaten von Amerika  
November 2023

IBM und das IBM Logo sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt und Servicennamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie unter [ibm.com/de-de/trademark](http://ibm.com/de-de/trademark).

Das vorliegende Dokument ist ab dem Datum der Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist.

Alle angeführten oder beschriebenen Beispiele illustrieren lediglich, wie einige Kunden IBM Produkte verwendet haben und welche Ergebnisse sie dabei erzielt haben. Die tatsächlichen Umgebungskosten und Leistungsmerkmale variieren in Abhängigkeit von den Konfigurationen und Bedingungen des jeweiligen Kunden. Es können keine generell zu erwartenden Ergebnisse bereitgestellt werden, da die Ergebnisse jedes Kunden allein von seinen Systemen und bestellten Services abhängen. Es liegt in der Verantwortung der Anwender, die Nutzbarkeit anderer Produkte oder Programme neben den Produkten und Programmen von IBM zu evaluieren und verifizieren.

DIE INFORMATIONEN IN DIESEM DOKUMENT WERDEN OHNE JEGLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GARANTIE ZUR VERFÜGUNG GESTELLT, EINSCHLIESSLICH DER GARANTIE DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER GARANTIE ODER BEDINGUNG DER NICHTVERLETZUNG VON RECHTEN.

Die Garantie für Produkte von IBM richtet sich nach den Geschäftsbedingungen der Vereinbarungen, unter denen sie bereitgestellt werden.

Erklärung zu bewährten Sicherheitsverfahren: Kein IT-System oder -Produkt sollte als vollkommen sicher angesehen werden, und kein einzelnes Produkt, kein Service und keine Sicherheitsmaßnahme kann eine missbräuchliche Nutzung oder einen missbräuchlichen Zugriff vollständig verhindern. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor böswilligem oder rechtswidrigem Verhalten von Dritten geschützt sind oder Ihr Unternehmen davor schützen.

