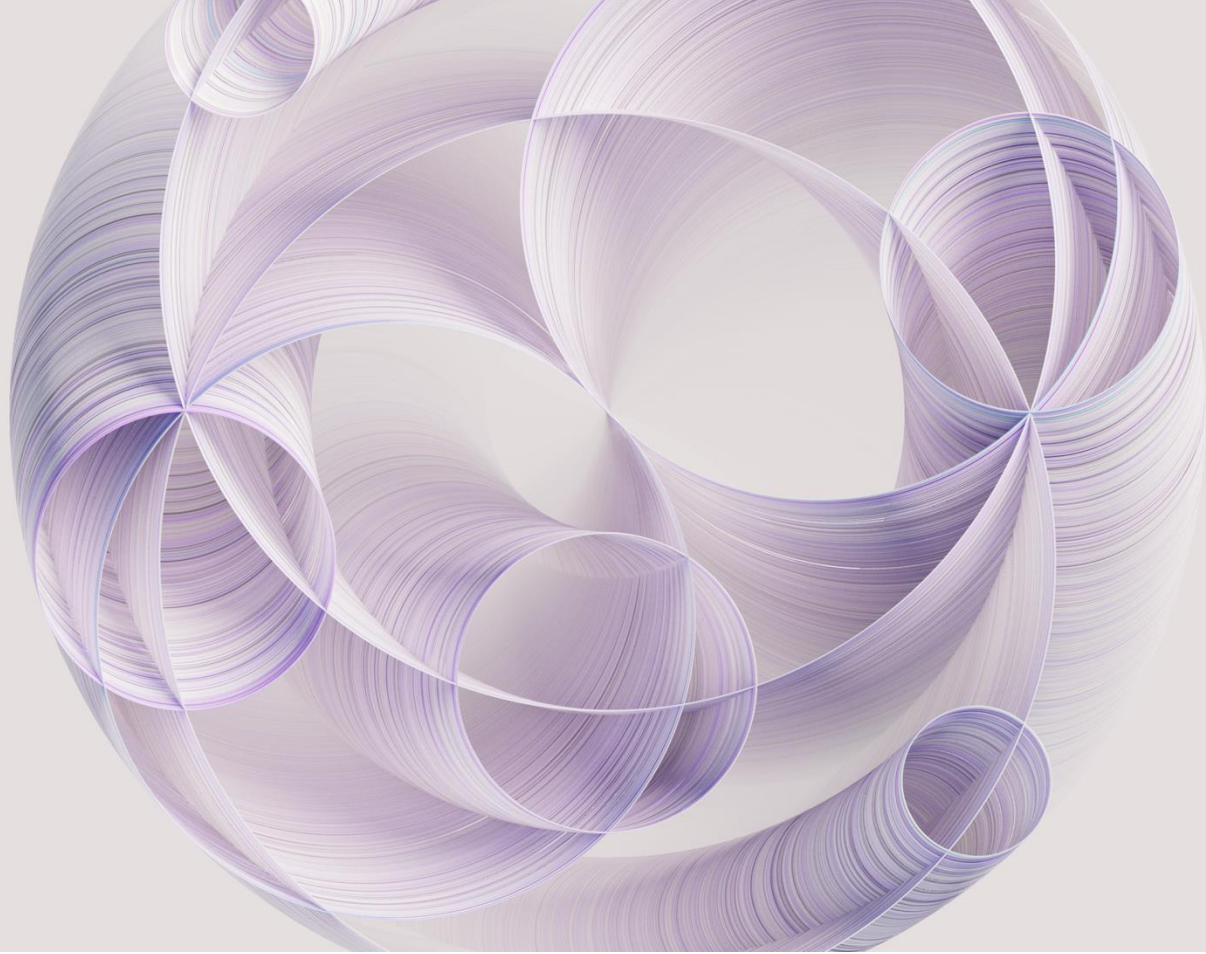


watsonx.governance  
Governing AI Agents



# Today's talk

Scale responsible AI with  
watsonx.governance

## 1

Governance is needed to scale AI with trust, compliance and security  
Reduce risk, bias, model drift, profanity and hate speech

---

## 2

Watsonx.governance is the leading AI governance solution

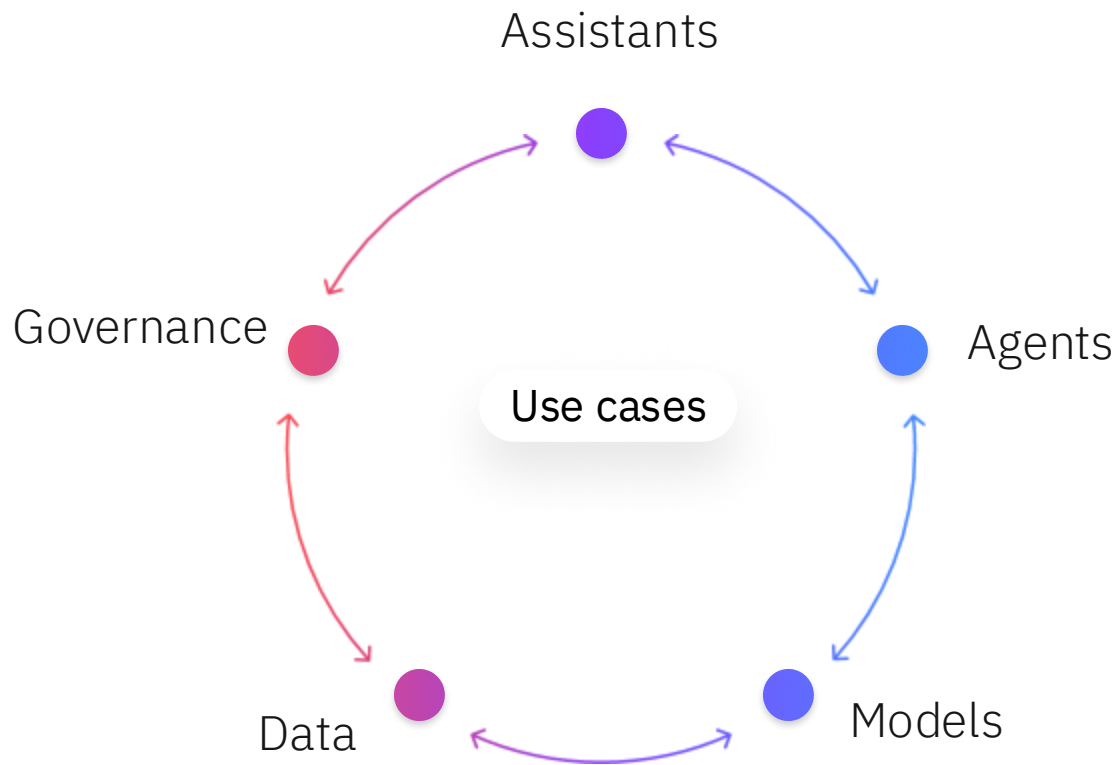
- Govern any AI, anywhere, without sacrificing speed and performance
  - Automate time consuming audit and documentation processes
- 

## 3

IBM's approach to data and AI

- Open, customized, multimodal and multi-model
- Both commercial and open-source innovation
- Customized to each business and use case to drive ROI

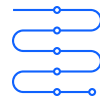
# AI building blocks to the future



AI agents can significantly enhance how effectively humans perform tasks and achieve business outcomes.



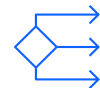
Augmenting human intelligence



Automating routine or time-consuming tasks



Improving efficiency and productivity



Enhancing decision-making and quality of responses

# Agentic AI brings with it immense promise

Opportunity

\$4.4T

global profits annually<sup>[1]</sup>

Expansion

45%

projected 5-year CAGR\* for the Agentic AI market <sup>[2]</sup>

Innovation

1/3

“By 2028, one-third of interactions with generative AI (Gen AI) services will use action models and autonomous agents for task completion, according to Gartner, Inc.” <sup>[3]</sup>

\*compound annual growth rate

<sup>1</sup> - [AI in the workplace: A report for 2025 | McKinsey](#)

<sup>2</sup> - [AI Agents: What They Are and Their Business Impact | BCG](#)

<sup>3</sup> - Gartner®, [Gartner Predicts One-Third of Interactions with Gen AI Services Will Use Action Models & Autonomous Agents for Task Completion by 2028](#), March 11, 2024

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Agents will power the future

By 2028, **one-third** of interactions with gen AI services will use **action models and autonomous agents** for task competition.<sup>1</sup>

1. [Gartner Predicts One-Third of Interactions with GenAI Services Will Use Action Models & Autonomous Agents for Task Completion by 2028](#), Gartner, March 11, 2024

As leaders look to scale generative AI, *trust* will be critical.



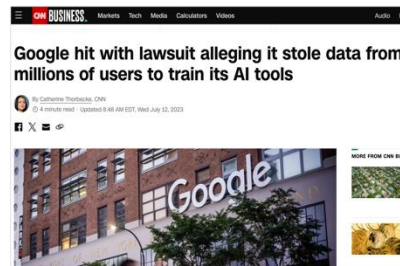
*New York Times sued OpenAI for the use of their copyrighted content. It is essential that data that drives GenAI is owned and safe to use from a legal standpoint.*



*Workday has faced many claims their AI tool used in hiring process is discriminatory. GenAI tools must be ethical and audited against racism, sexism and other prejudices.*



*DPD, a UK-based parcel delivery service discontinued its AI Chatbot after a frustrated user coaxed the system into speaking bad about DPD's customer service. GenAI needs to be consistent and avoid coercion from users to change.*



*Google was sued for creating GenAI tools based on the data collected by its users without the knowledge that their data would be used in this way. Transparency of data is needed for both the collection and distribution of GenAI data.*

# Assess, evaluate and monitor across agentic AI

## Agentic AI Governance

Evaluate, deploy and monitor all types of agents.

Manage compliance, security and risk.



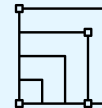
## Orchestrator for Tools and Agents

Multi-agent, multi-tool supervisor, router, and planner which facilitates complex task execution



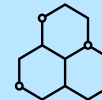
## Prebuilt AI Agents

Accelerate AI Agents with pre-built utility agents and domain agents. Provide a searchable catalog of AI agents and tools.



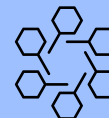
## Build Your Own Agents

Build custom designed agents with no-code and pro-code tooling. Integrate 3<sup>rd</sup> party agents built in any tool or framework



## AI Agent Ops

Discover, manage, monitor and optimize autonomous AI agents





Your AI for  
business strategy  
can't succeed  
without AI  
governance



Changing  
regulations



Multiple  
stakeholders



Manual, error-prone  
documentation



Increased risk



Disparate tools  
and data



Vulnerable data

# AI needs governance



The process of directing,  
monitoring and managing the AI  
activities of an organization  
through automation

# Your AI for business strategy can't succeed without AI governance



Changing regulations



Multiple stakeholders



Manual and error prone  
documentation



Increased risk

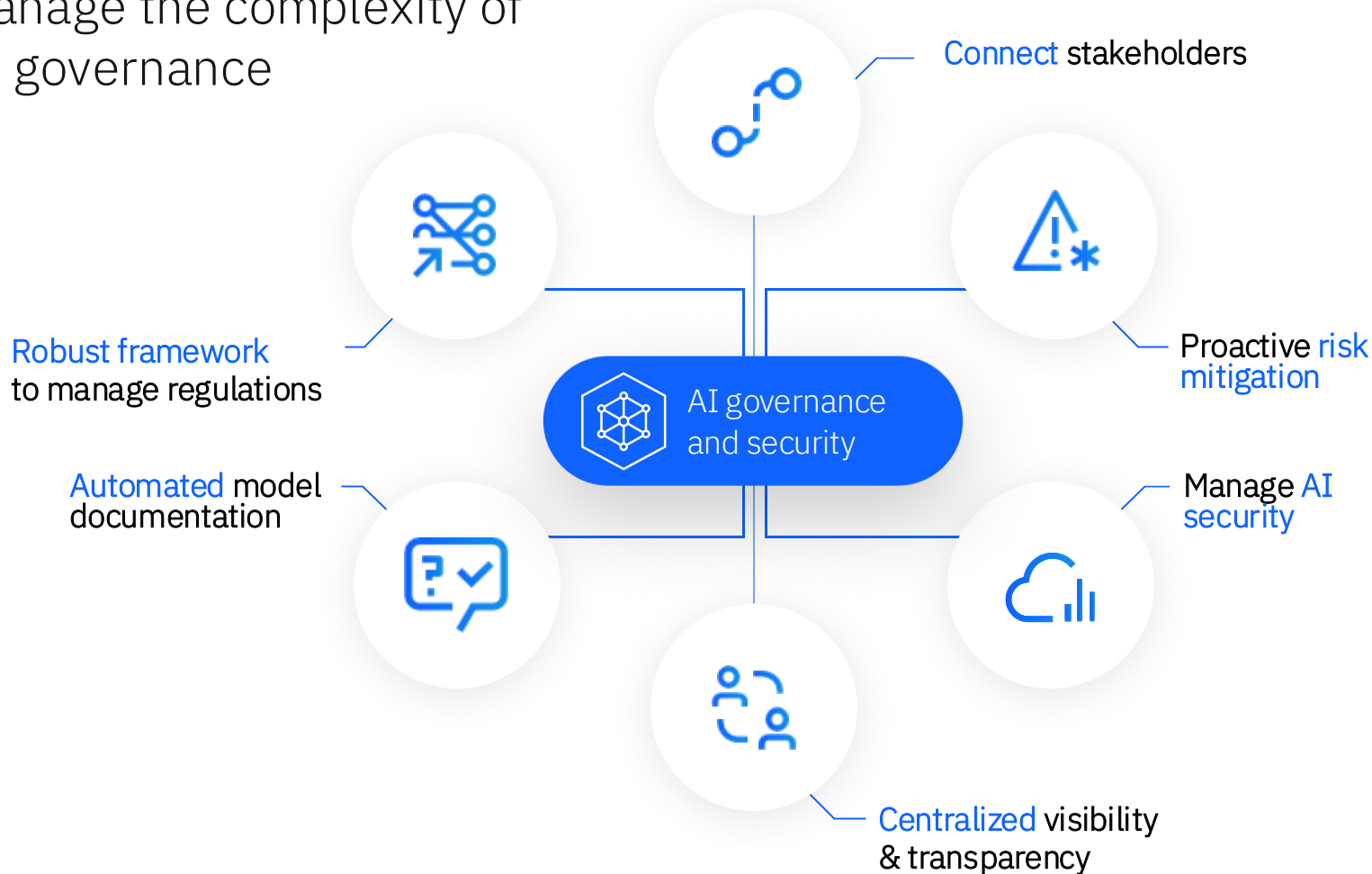


Disparate tools  
and data



Vulnerable data

# Manage the complexity of AI governance



Put AI to work with **watsonx**.

IBM watsonx is a portfolio of AI products that accelerates the impact of generative AI in core workflows to drive productivity.

# watsonx

A portfolio of AI products that accelerates the impact of generative AI in core workflows to drive productivity.

## watsonx.ai

Enterprise-grade AI studio that helps AI builders innovate with all the APIs, tools, models, and runtimes to build AI solutions

Featuring **IBM Granite**, and popular third-party models including **Mixtral**, **Llama** series

## watsonx.data

The **hybrid, open data lakehouse** to power AI and analytics with all your data, anywhere

## watsonx.governance

End-to-end toolkit for AI governance to manage **risk and compliance across the entire AI lifecycle**.

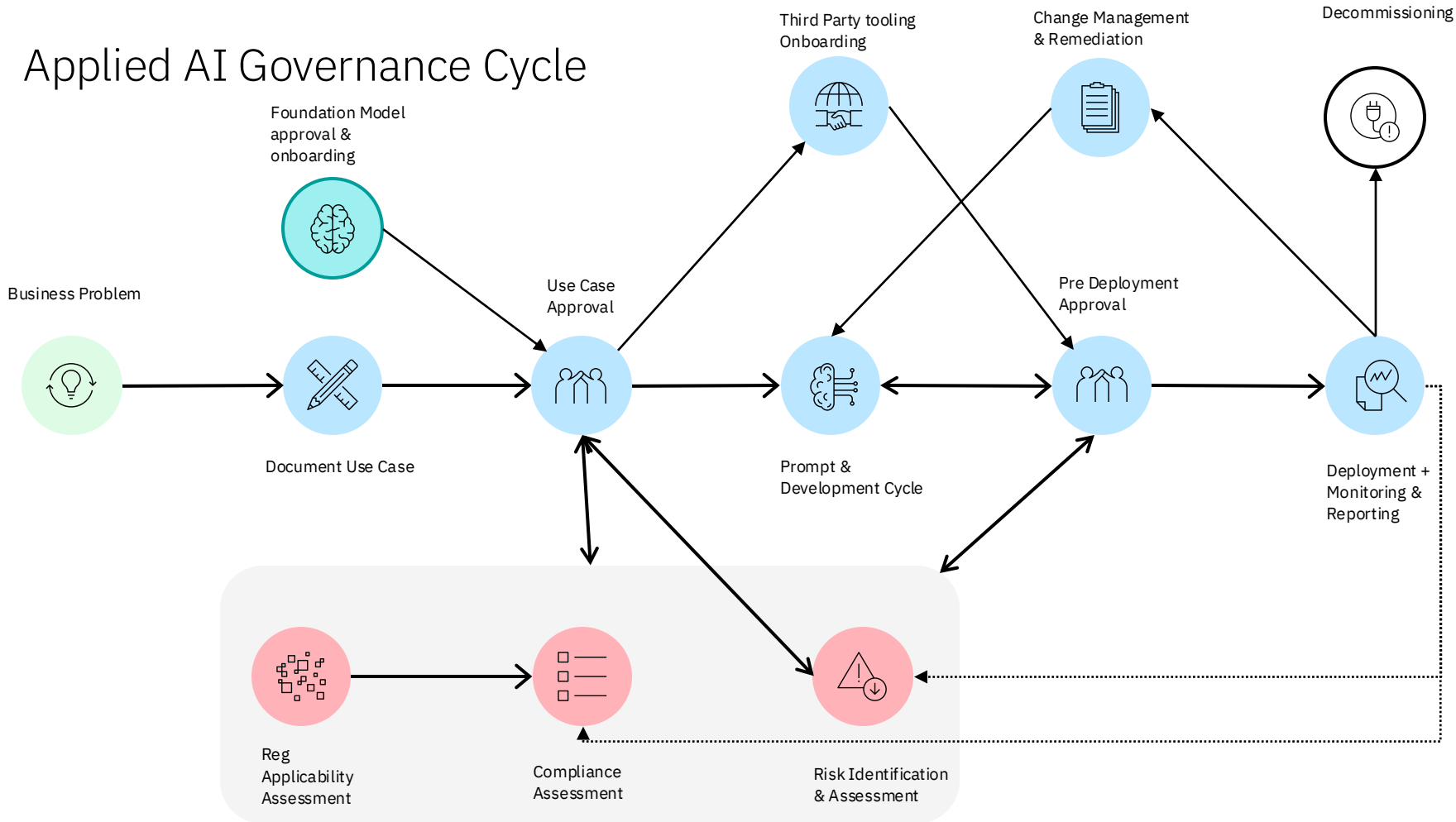
## watsonx Orchestrate

An enterprise-ready solution that helps create, deploy, and manage AI assistants and agents to automate processes and workflows.

## watsonx Code Assistant

Accelerate development, **application modernization**, and assist with IT Operations

# Applied AI Governance Cycle



IBM watsonx.governance

Accelerate responsible,  
transparent and explainable  
AI workflows



Centralized  
AI lifecycle governance

Manage, monitor and govern  
any AI: model, app, agent or  
tool; across IBM and 3<sup>rd</sup> party  
like OpenAI, AWS, Azure, GCP,  
Meta, etc.



Proactive  
AI risk and security  
management

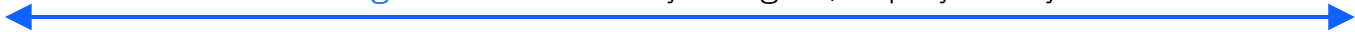
Proactively detect and  
mitigate AI risks, evaluate  
AI assets, and secure AI  
deployments with Guardium  
AI security



Trustworthy  
and dynamic  
compliance

Manage AI for safety  
and transparency with  
our regulatory library,  
automation and  
industry standards

Platform agnostic: Govern any AI Agent, deployed anywhere



SAP SuccessFactors



SAP Ariba

workday.



zoominfo

Seismic



servicenow



coupa

dun & bradstreet



# watsonx.governance at a glance



- AI use case owners
- Data Scientist / AI Engineers
- Model validators
- Audit teams
- Compliance teams
- Risk management teams
- AI Security teams



- Data engineers
- AI Engineers
- (Citizen) data scientists
- MLOps
- ML engineers

## Lifecycle governance

## Risk management

## Regulatory compliance

### AI risk governance and security

Model inventory | Risk assessments | Workflows | Dashboards | Issue management



### AI Factsheet

Capture model facts throughout the lifecycle



### AI Observability and Guardrails

Model health | Harmful content detection | Accuracy | Drift | Bias | Explainability



## Build and Deploy

IBM watsonx.ai | AWS | MS Azure | GenAI apps | SaaS solutions | Other



# AI lifecycle governance



## Key Highlights

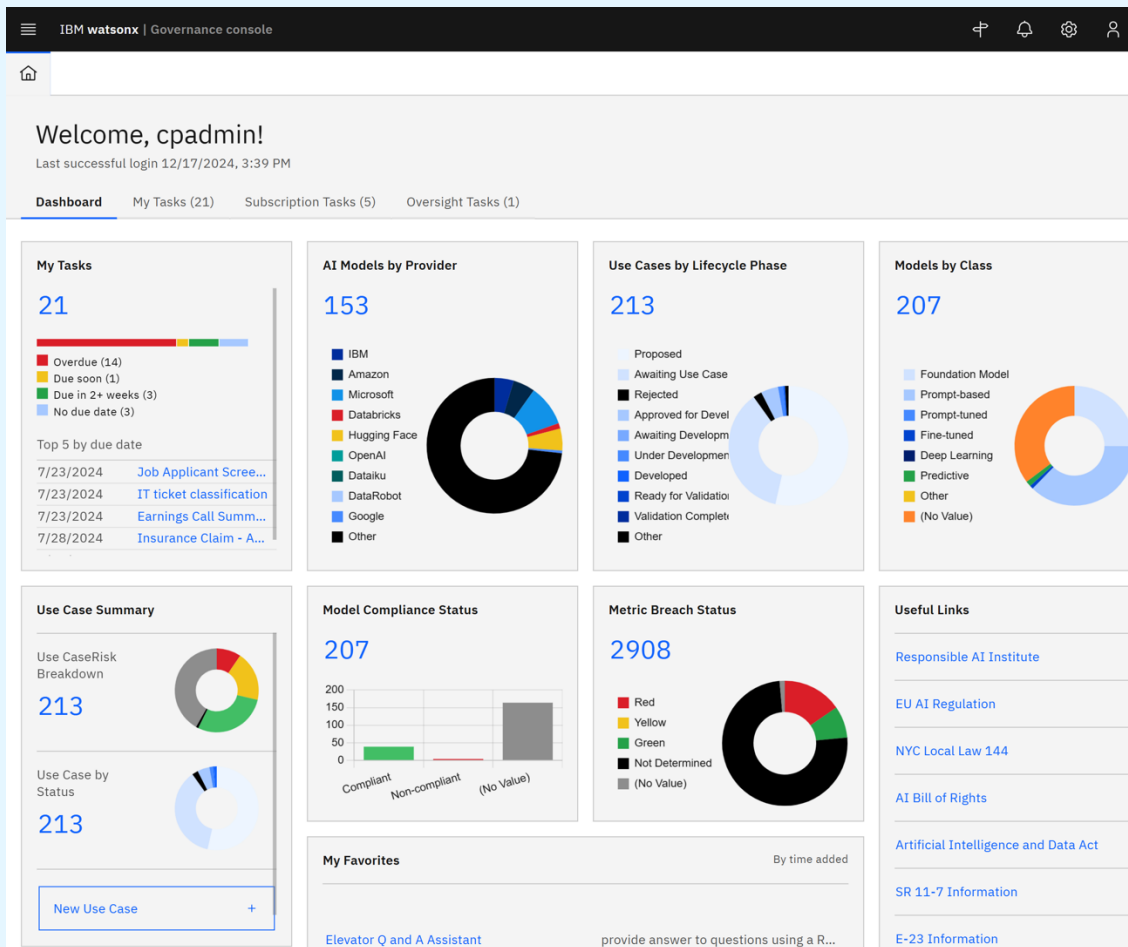
- Inventory and track ML models, GenAI apps and agents from concept/ideation through lifecycle
- Evaluate and assess your GenAI prompt templates, ML models, agents during build
- Automate the capture of the model, app and agent metadata to facilitate management and compliance

## Solves for:

1. Time-consuming documentation
2. Manual or non-systematic approach to evaluate prompts
3. Lack of transparency through lifecycle

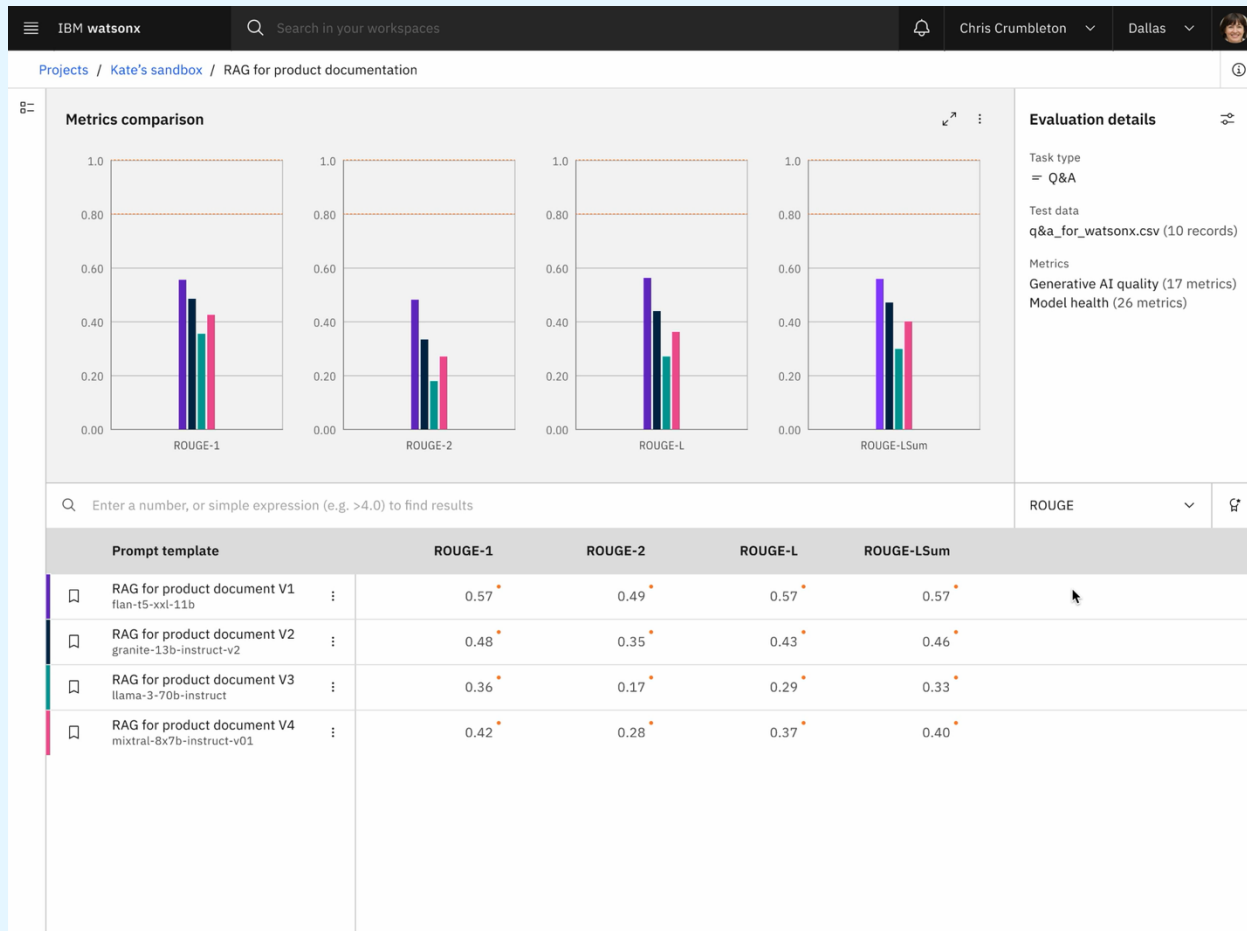
Scale responsible AI with watsonx.governance

## Bring transparency and visibility into your AI use cases





**Example:** Accelerate AI asset selection as you build with easy comparative evaluation on multiple quality metrics in Evaluation Studio



# Proactive and efficient risk management



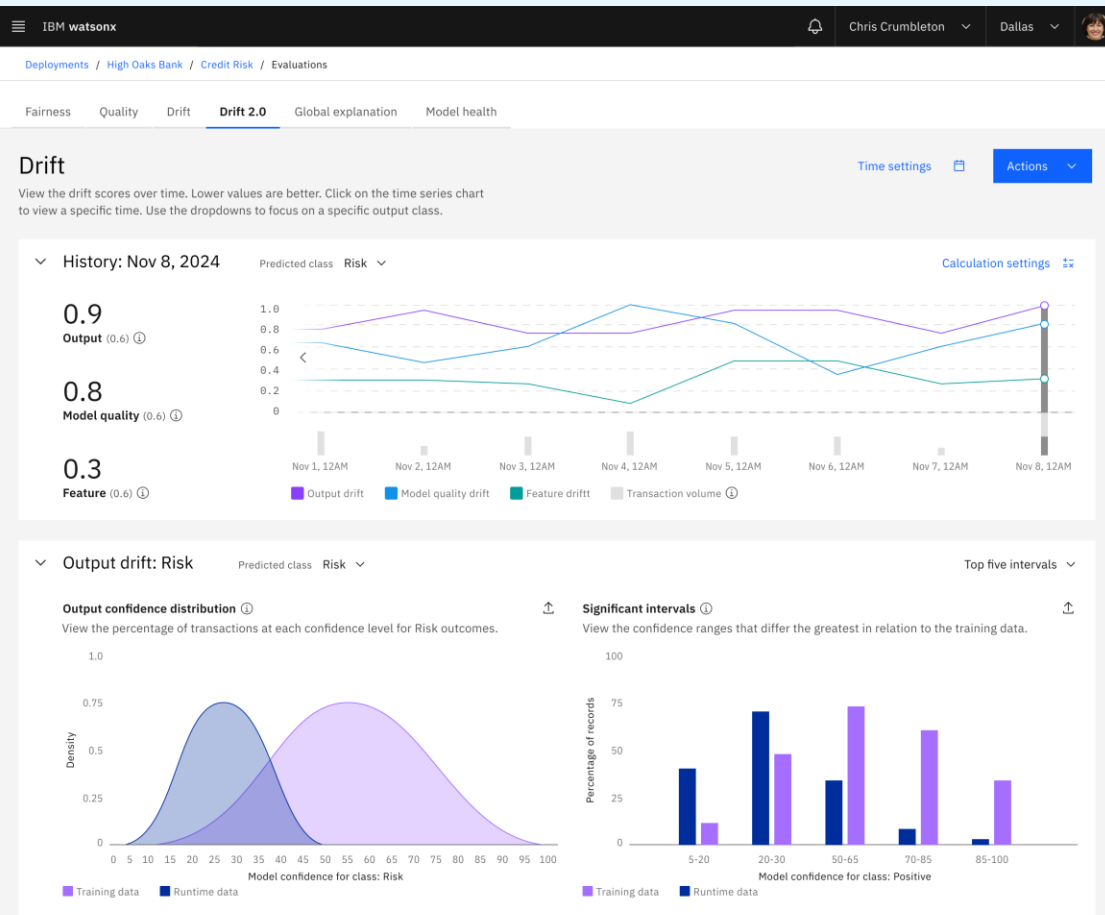
## Key highlights

- Identify and manage AI risks early on with risk assessments at use case and model-level
- Mitigate risks and moderate content with Guardrails
- Observe and understand with continuous monitoring with alerts and explainability

## Solves for:

1. Limited visibility across AI use cases
2. Lack of risk management for AI
3. Identifying potentially harmful content in prompts

## Assess, identify, and manage AI risk



watsonx.governance for  
proactive and efficient  
risk management



**Example:** identify potential risks and mitigation for AI use cases early on with out-of-the-box AI risk assessments and applied AI risk taxonomy

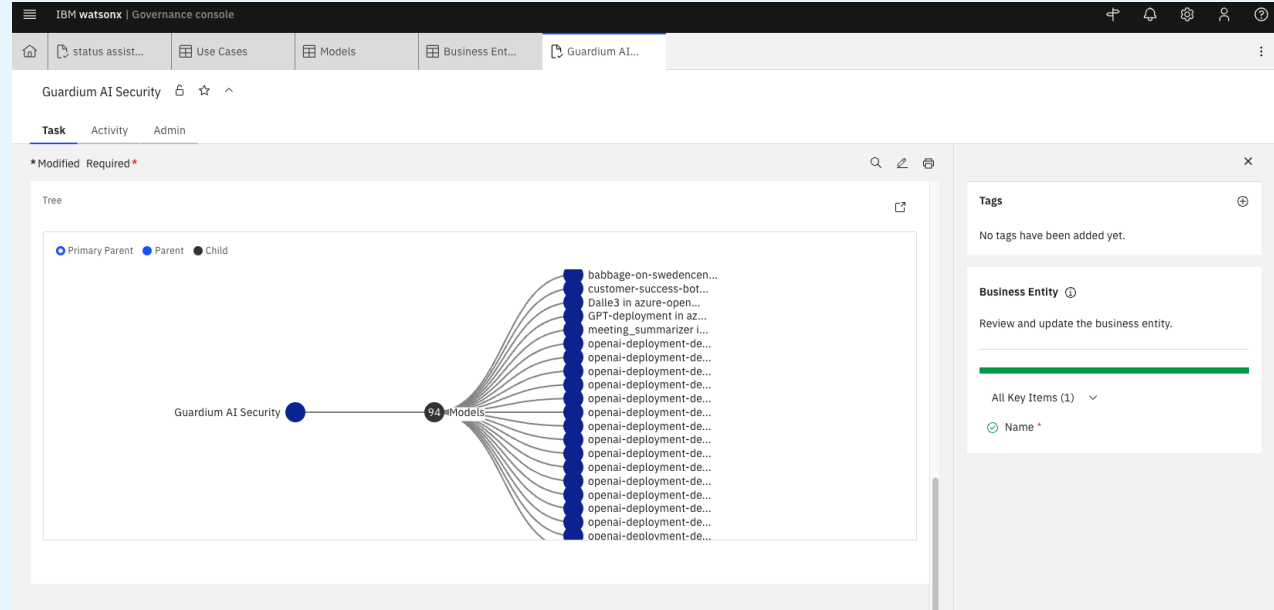
Manage **risk and compliance** at scale

## IBM Guardium AI Security integrates with watsonx.governance for Trusted AI

### Key highlights

- Discover AI models, data, and applications used by an organization across AI Services and enrich watsonx.governance use case inventory
- Automatically identify unregistered AI deployments and trigger the appropriate governance workflow
- Operationalize across product, risk, compliance, and security stakeholders

Govern, secure and monitor AI in one unified experience with Guardium AI Security and watsonx.governance integration



Discovered models grouped in same business entity

# Dynamic and trustworthy compliance



## Key highlights

- Ingest and represent internal and external AI regulations to present to use case owners and compliance officers
- Provide ability to record and assess AI Use case evidence for audit and compliance
- Use Factsheets for transparent model processes

## Solves for:

1. Changing regulations
2. Inaccurate documentation

## Meet growing AI regulatory landscape

The screenshot displays the IBM watsonx Governance web application. The top navigation bar includes the IBM watsonx logo, a notification bell, and user information for Chris Crumbleton in Dallas. The breadcrumb trail shows the path: Deployments / High Oaks Bank / Credit Risk / Evaluations. The main interface is divided into a left sidebar and a main content area. The sidebar lists various governance categories: Governance (selected), Foundation model, Prompt template, Prompt parameters, Evaluation, Develop (with sub-items Finance and Test), Validate, Operate, Additional details, Attachments, Charts, and Files. The main content area displays the 'Credit Risk Model' factsheet. It includes the AI use case name 'Credit Risk Model', a draft ID 'e98cf678-37bc-4ef7-827-02cf70186112', a description of machine learning models for loan risk assessment, and a 'Read more' link. Below this, the 'Approach' section shows 'Default approach' as the selected version (0.0.1), with a description of its purpose for tracking AI assets. The 'Lifecycle' section at the bottom shows three stages: 01 Develop, 02 Validate, and 03 Operate, each with an icon representing its phase.



**Example:** assess regulatory applicability  
for your GenAI use cases

IBM watsonx

AskHR Chatb...

Use Case

AskHR Chatbot

Status

Awaiting Use Case Approval

Risk Level

Actions

Task

Activity

Admin

\*Modified Required\*

General

Name

AskHR Chatbot

Description

Provide HR policy and operational responses to IBM employees

Owner

Ian Francis

Status

Awaiting Use Case Approval

Use Case Type

Purpose

Provide HR policy and operational responses to IBM employees

Risk Level

Third Party Link

Use Case Details

Uses Foundation Models

Yes

Externally Facing

No

Proposed Solution

AI Infused assistant adopting a RAG approach with multiple model selection

Target Implementation Date

6/30/2024

Additional Details

Stakeholders and Approvals



# Agentic AI

## Risks and Challenges



### New

Emerging areas *intrinsic* to agentic AI

#### Risks

- Unsupervised autonomy
- Data bias
- Redundant actions
- Attack on AI agent's external resource
- Tool choice hallucination
- Sharing IP/PI/confidential information

#### Challenges

- Reproducibility
- Traceability
- Attack surface expansion
- Harmful and irreversible consequences



### Amplified

Known areas *intensified* by agentic AI

#### Risks

- Misaligned actions
- Discriminatory actions
- Over- or under-reliance
- Unauthorized use
- Exploit trust mismatch
- Unexplainable or untraceable actions
- Lack of transparency

#### Challenges

- Evaluation
- Accountability
- Compliance
- Mitigation and maintenance
- Infinite feedback loops
- Shared model pitfalls

# Key lifecycle governance activities

## For agentic systems



### Experimentation tracking

Track agentic app variants and compare results to inform which to push to production



### Agentic system metrics, monitoring and alerts

Oversee elements such as hallucination, answer relevance, and system drift in production and development



### Traceability

Help developers debug agentic app by tracing each step of the user interaction and agent processing



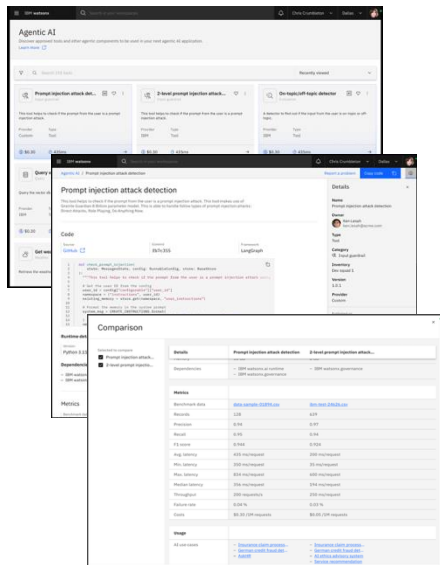
### Cataloging of agentic AI applications

Single consolidated view of all in development and use

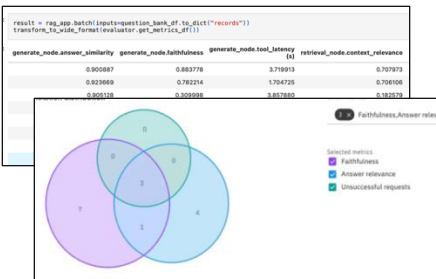
# Agentic AI governance feature highlights\*

# Providing the tools and capabilities to develop, deploy, manage and govern AI agents

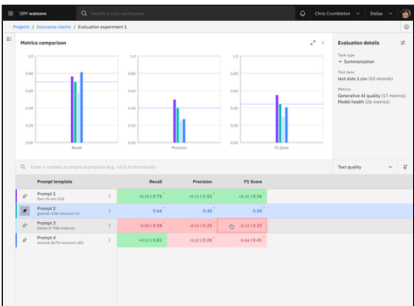
## Agentic tool catalog



## Agent evaluators



## Agent evaluation studio



## Agent production monitoring\*\*



\*Please note: roadmap items are subject to change  
\*\*Release planned for Q3 2025

# watsonx.governance

## Governance of agentic AI

### Agent Onboarding

- *Onboard Agents, assess risk, and capture metadata from build to deployment*
- **AI Risk Assessment** identifies AI agent risks during onboarding with automated workflows
- **Stakeholder management** fosters cross-functional collaboration to approve and onboard agents
- Identify and manage AI Risks by using automated workflows to onboard AI Agents
- Identify risk levels and applicable AI regulations for your AI use case

### Key features:

- Create an AI use case describing your business goal using the Governance Console
- Risk questionnaire to identify risk dimensions, compliance needs, and applicable AI regulations and generate an assessment for your use case

The image displays two screenshots of the Watsonx Governance console, illustrating the AI Risk Assessment process.

**Top Screenshot: Agent Onboarding Risk Identification (AGENT-0000025)**

This screen shows the 'Agent Onboarding Risk Identification' workflow. It includes a 'Main Section' with a 'Training Data Risk' section. The 'Training Data Risk' section contains a 'Training Data Risk' section with a 'Training Data Risk' section. The 'Training Data Risk' section contains a 'Training Data Risk' section.

**Bottom Screenshot: User Chatbot**

This screen shows the 'User Chatbot' interface. It includes a 'Main Section' with a 'Training Data Risk' section. The 'Training Data Risk' section contains a 'Training Data Risk' section. The 'Training Data Risk' section contains a 'Training Data Risk' section.

Name	Description	Progress (%)	Tags
AI Risk Identification (User Chatbot)	AI use case risk identification assessment (2025-04-02)	100	

Name	Description	Inherent Risk Rating	Residual Risk Rating	Status	Tags
Personal information in prompt	Personal information or sensitive personal information that is included as a part of a prompt that is sent to the model.	Medium	Low	Approved	
Output bias	Generated content might unfairly represent certain groups or individuals.	Medium	Low	Approved	
Hallucinations	Hallucinations generate factually inaccurate or untruthful content with respect to the model's training data or input. This is also sometimes referred to as lack of faithfulness or lack of groundedness.	High	Medium	Approved	
Toxic output	Toxic output occurs when the model produces hateful, abusive, and profane (SWAP) or obscene content. This also includes behaviors like bullying.	High	Medium	Approved	
Harmful output	A model might generate language that leads to physical harm. The language might include overtly violent, covertly dangerous, or otherwise indirectly unsafe statements.	Medium	Low	Approved	
Incomplete advice	When a model provides advice without having enough information, resulting in possible harm if the advice is followed.	High	High	Approved	

## Agent onboarding demo (1 min)

IBM watsonx

Search in your workspaces

Adam Anderson

Dallas

User Chatbot

User Case

User Chatbot ☆ ^

Status

Under Development

Risk Level

Medium

Actions

Task

Activity

Admin

Security Performance Monitoring

\*Modified Required \*

🔍 ✎ ⌘ 🖨

×

General ⓘ

^

Name \*

User Chatbot

Use Case Type

AI

Status

Under Development

Description

A chat assistant that can help users by answering their questions.

Owner

Bob Eldridge

Purpose

Question answering

Stakeholder Departments

Legal Engineering CTO Ethics

Technical Owner

Mel Diaz

Third Party Link

Use Case Details ⓘ

^

Uses Generative AI

Yes

Externally Facing

Yes

Target Implementation Date

4/25/2025

Proposed Solution

An Agentic RAG application

Additional Details

Data Gathering Completion Date

4/2/2025

Risk ⓘ

^

## Agentic Tool Catalog

*Consolidated list of agentic tools to manage and inform selection*

- **Re-using agent tools** helps accelerate progress across users and use cases
- **Promote approved tools** to encourage utilization and proper use
- Tools perform specific tasks and are key in designing and building agentic systems and span a broad range e.g. data retrieval, external connection tools, and more.
- Tool catalogs are a way to manage tool ‘sprawl’ and help bring consistency across teams/units

### Key features:

- Tool lineage by mapping tools to use cases
- Search by use case type / domain to find tools and get started faster
- Filter tools available by type of tool
- Tool card that documents purpose of the tool, along with quality metrics
- Easy side-by-side comparison of various tools
- See tool ratings from other users

The screenshot displays the 'Agentic AI' tool catalog in the Watsonx Governance console. The interface is divided into several sections:

- Tool Cards:** A grid of tool cards, each representing a different agentic tool. Visible tools include:
  - Prompt injection attack detector...**: A tool to check if the prompt from the user is a prompt injection attack. Provider: Custom, Type: Tool, Rating: 4.0/5.0.
  - 2-level prompt injection attack...**: A tool to check if the prompt from the user is a prompt injection attack. Provider: IBM, Type: Tool, Rating: 4.0/5.0.
  - On-topic/off-topic detector**: A detector to find out if the input from the user is on-topic or off-topic. Provider: IBM, Type: Tool, Rating: 4.0/5.0.
  - Query vector DB**: Query the vector db to fetch data related to the user query. Provider: IBM, Type: Tool, Rating: 4.0/5.0.
  - RAG answer generation**: Generate an answer for a user question using the provided context. Provider: IBM, Type: Tool, Rating: 4.0/5.0.
  - SQL-Turbo image generat...**: Generate images from text with the SQL-Turbo model. Provider: IBM, Type: Tool, Rating: 4.0/5.0.
- Tool Card Detail View:** A detailed view of the 'Prompt injection attack detection' tool. It includes:
  - Description:** This tool helps to check if the prompt from the user is a prompt injection attack. This tool helps to check if the prompt from the user is a prompt injection attack. This tool helps to check if the prompt from the user is a prompt injection attack.
  - Code:** A code editor showing the tool's implementation in Python.
  - Metadata:** Information about the tool, including its name, version, and provider.
  - Dependencies:** A list of tools or services that this tool depends on.
  - Metrics:** A table showing the tool's performance metrics.
- Comparison View:** A side-by-side comparison of the 'Prompt injection attack detection' tool and the '2-level prompt injection attack...' tool. It includes a table with the following data:

Metric	Prompt injection attack detection	2-level prompt injection attack...
Standard data	Blue-watsonx-Metric	Blue-watsonx-Metric
Records	125	125
Precision	0.78	0.97
Recall	0.91	0.91
F1 score	0.84	0.94
Avg latency	100 ms/req	100 ms/req
Max latency	300 ms/req	300 ms/req
Max memory	100 MB/req	100 MB/req
Max tokens	100 tokens/req	100 tokens/req
Throughput	250 req/s	250 req/s
Peak usage	0.14%	0.14%
Cost	\$0.001/req	\$0.001/req

## Agentic Tool Catalog Demo (1 min 15 secs)

The screenshot displays the IBM watsonx Agentic Tool Catalog interface. At the top, the header includes the IBM watsonx logo, a search bar for workspaces, and user information for Adam Anderson in Dallas. The main section is titled "Agentic components" with a subtitle "Discover approved tools and other agentic components to be used in your next agentic AI application." and a "Learn more" link. Below this is a search bar for 193 tools and a "Recently viewed" dropdown. The tools are presented in a grid of six cards, each with an icon, title, description, provider, type, cost, and execution time.

Tool Name	Icon	Category	Description	Provider	Type	Cost	Time
Prompt injection attack det...	Shield with 'X'	Input guardrail	This tool helps to check if the prompt from the user is a prompt injection attack.	Custom	Tool	\$0.30	435ms
2-level prompt injection attack...	Shield with 'X'	Input guardrail	This tool helps to check if the prompt from the user is a prompt injection attack.	IBM	Tool	\$0.30	435ms
Answer relevance	Search icon	Evaluation	Measure the relevance of AI-provided answers.	IBM	Tool	\$0.30	435ms
Webcrawler	Database icon	Internet	Retrieve information from a website.	IBM	Tool		
DuckDuckGo search	Duck icon	RAG	Retrieve information from the internet with the DuckDuckGo search engine.	IBM	Tool		
Document search	Document icon	Text-to-image	Search documents with vector indexes.	Custom	Tool		

# watsonx.governance

## Governance of agentic AI

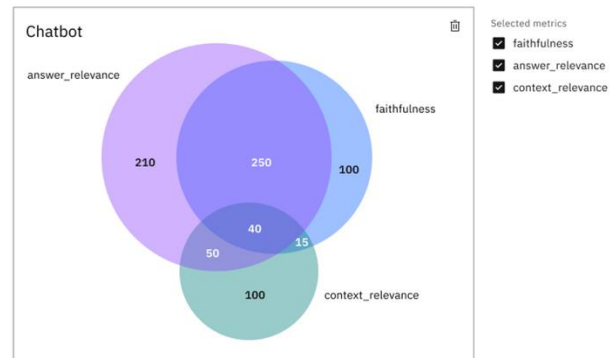
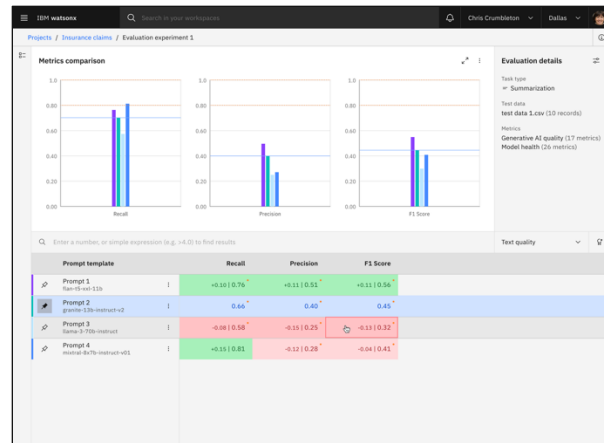
### Agent Evaluators and Evaluation Studio

*Help organizations understand and improve agents' performance to scale with confidence*

- **Evaluation metrics** assess agent competence for various tasks
- **Root cause analysis** identifies underlying reasons for poor performance to inform improvements
- Developers will be able to easily leverage the 50+ evaluation metrics from watsonx.governance to evaluate their tools and use the computed metrics in their agentic AI application
- Developers can run experiments to compare results and select the best performing version

#### Key features:

- Compute metrics to evaluate the application by adding a one-line decorator
- Identify root cause for poor performance using Venn charts to understand interactions between metrics and make necessary improvements
- Use Evaluation Studio to track and compare experiments





## Agent Evaluation Demo (2 mins)

IBM watsonx Search in your workspaces Adam Anderson Dallas

Projects / Agentic AI / Advanced notebook for IBM watsonx governance evalua

File Edit View Run Kernel Help Memory:197 / 8192 MB Python 3.11

### Set up the local vector store

We have created a local vector store comprising of a few medium posts by [Manish Bhide](#) and [Ravi Chamarthi](#). These posts focus on the various capabilities in IBM watsonx.governance (and erstwhile IBM Watson OpenScale). Hence, our queries will focus on these capabilities covered in the above posts.

For user's convenience, the vector store has been compressed. The following cell downloads the compressed file, extracts it locally, and initializes the Chroma store.

```
In [2]: %rm medium_db.zip
        %rm -r medium_db/

        !wget https://github.com/IBM/ibm-watsonx-gov/raw/refs/heads/samples/notebooks/data/agentic/medium_db.zip

rm: medium_db.zip: No such file or directory
rm: medium_db/: No such file or directory
--2025-03-28 14:59:59-- https://github.com/IBM/ibm-watsonx-gov/raw/refs/heads/samples/notebooks/data/agentic/medium_db.zip
Resolving github.com (github.com)... 20.207.73.82
connected to github.com (github.com)[20.207.73.82]:443...
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/IBM/ibm-watsonx-gov/refs/heads/samples/notebooks/data/agentic/medium_db.zip [following]
--2025-03-28 14:59:59-- https://raw.githubusercontent.com/IBM/ibm-watsonx-gov/refs/heads/samples/notebooks/data/agentic/medium_db.zip
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
connected to raw.githubusercontent.com (raw.githubusercontent.com)[185.199.108.133]:443...
HTTP request sent, awaiting response... 200 OK
Length: 1203223 (1.1M) [application/zip]
Saving to: 'medium_db.zip'

medium_db.zip      100%[=====>] 1.15M  4.34MB/s   in 0.3s

2025-03-28 15:00:00 (4.34 MB/s) - 'medium_db.zip' saved [1203223/1203223]

In [3]: import zipfile

        with zipfile.ZipFile("medium_db.zip", "r") as zip_ref:
            zip_ref.extractall(".")

In [4]: from langchain_chroma import Chroma
        from langchain_openai import OpenAIEmbeddings

        openai_embed_model = OpenAIEmbeddings(model="text-embedding-3-small")

        vector_store = Chroma(
            collection_name="medium_articles",
            embedding_function=openai_embed_model,
            persist_directory="/medium_db"
```



## Differentiation:

Accelerate responsible, transparent and explainable AI for both gen AI and ML models across any public or private cloud.



**Govern any model, agent or AI app anywhere**

Apply governance to ML and gen AI—open or closed—IBM and third parties (like OpenAI, AWS, Meta).



**Assess and reduce AI risk at runtime**

Continuous monitoring and recommendations with model risk assessment and real-time alerts.

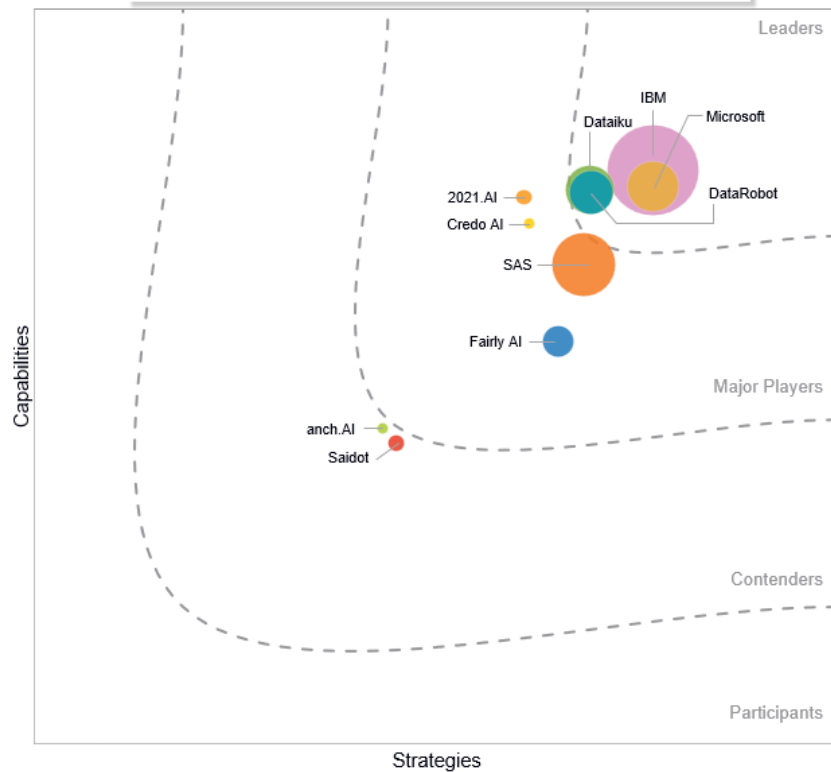


**Worldwide compliance expertise**

Compliance with internal policies, industry standards, and AI regulation, with automated audit processes.

# IBM is a leader in AI Governance and ML Ops

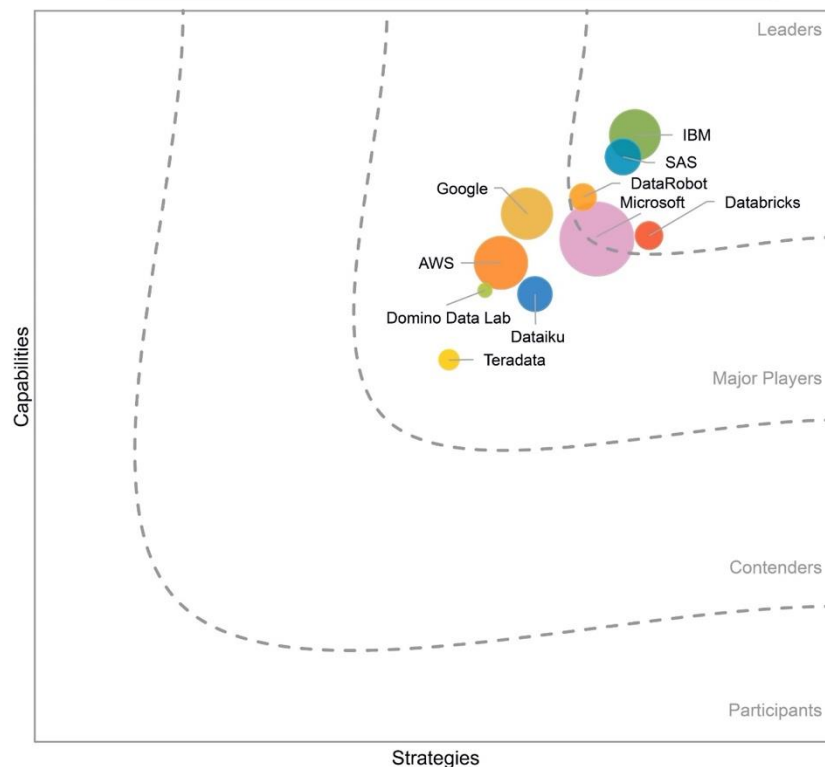
IDC MarketScape Worldwide AI Governance Platforms, 2023



Source: "IDC MarketScape: Worldwide AI Governance Platforms 2023 Vendor Assessment"

**Key strengths:** end-to-end solution and commitment to support

IDC MarketScape Worldwide Machine Learning Operations Platforms, 2024



Source: IDC, 2024

Source: "IDC MarketScape: Worldwide Machine Learning Operations Platforms 2024 Vendor Assessment" November 2024, IDC # US51573824

**Key strengths:** AI governance, no-code/low-code options and flexible deployment

For more information  
on IBM's perspective

Read *AI agents:  
Opportunities, risks, and  
mitigations*, a deep-dive into  
the unique risks posed by AI  
agents and potential  
mitigations, written by the  
IBM AI Ethics Board.

Scan the QR code to  
access the paper:

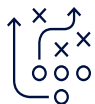


## **AI agents:** Opportunities, risks, and mitigations



# Three ways to get started with watsonx today

## Looking forward to today's discussions



### Free trial

Core watsonx features to start building AI models and accessing data across your organization.



### Request a client briefing or demo

Discussion and custom demonstration of IBM's generative AI watsonx point of view and capabilities. Understand where generative AI can be leveraged now for impact in your business.

2-4 hours onsite or virtual



### 5-year business value assessment

Engagement with an IBM multi-disciplinary team to jointly innovate and rapidly prove the business value of generative AI solutions using watsonx.

1-4 weeks

