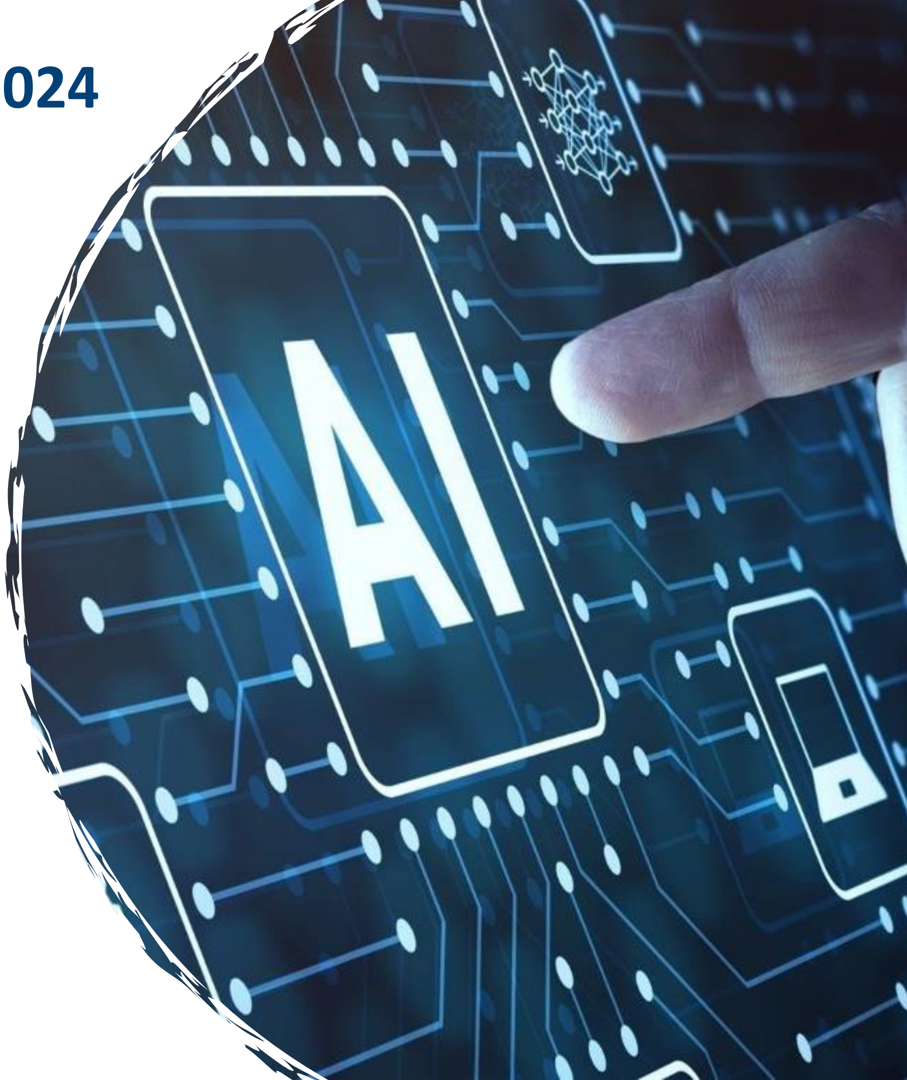
ETSI

The Standards People

ETSI AI Conference 2024



An Enterprise Software Framework to Manage AI Governance at Scale

Presented by:

Martijn Wiertz
EMEA Technical Sales Lead, AI governance
martijnwiertz@nl.ibm.com

February 7th, 2024

AI governance

A system of rules, practices, processes and tools that help an organization

→ use AI in alignment with its values and strategies

→ address compliance requirements

→ drive trustworthy performance

Generative AI and applications, like OpenAI's ChatGPT, make AI governance a necessity, as using pretrained AI models billions of times sharpens risk concerns.

Gartner – Hype Cycle for Data and Analytics Governance, 2023

Data & Trust Alliance, IBM – The urgency of AI governance, 2023
https://dataandtrustalliance.org/news/perspectives-from-the-front

Rapid evolution in AI drives evolution in the governance of AI

Generative AI

65/35

Split in software spend on non-generative AI (65%) and generative AI (35%). [1]

36

Amplified and new risk with generative AI. [2]

Govern both forms of AI in a consistent manner.

Extend your governance to account for the new aspects of generative AI.

Innovation in models

~5000

New foundation models posted on Hugging Face every week.

Continuous innovation in open source and commercial offerings gives you an increasing range of options and trade-offs.

Govern the onboarding of new models.

Govern the trade-offs in use cases.

Consumption models

60/40

Split in software spend on AI platforms (60%) and AI embedded in enterprise applications (40%). [1]

70%

Of independent software vendors will have embedded generative AI capabilities. [1]

Govern all AI, regardless of how and it's created or consumed.

Legislation

200+

Pages in the EU AI Act.

10

Standardization requests in the EU AI Act.

Translate your responsibilities into controls and workflows.

Risk-assess your use cases.

Adopt technical standards.

[1] Gartner – Forecast Analysis: AI Software. 2023-2027, Worldwide
[2] IBM AI Risk Atlas

Elements of AI risk

Accountability

Accuracy

Fairness

Truthfulness

Transparency

Drift

Trusted data

Sustainability

Explainability

Adversarial Robustness

IP/PII leakage

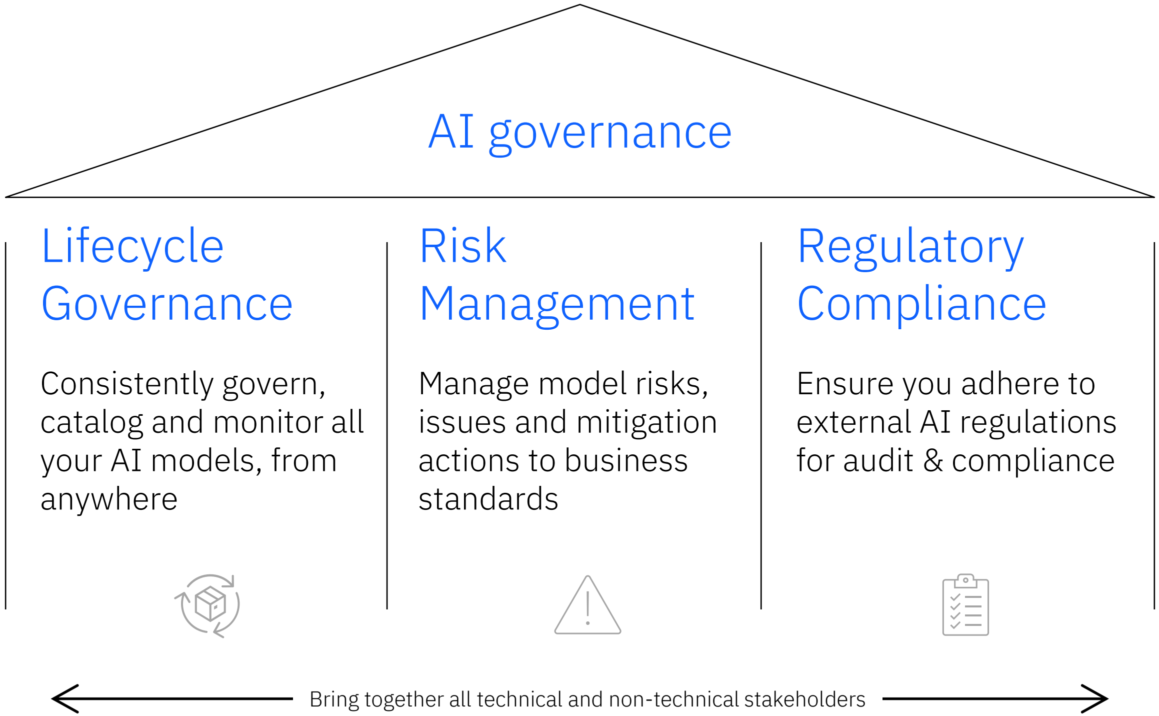
...

Regulatory Risk

Reputational Risk

Operational Risk

Three pillars of AI governance



AI governance

Lifecycle Governance

Consistently govern, catalog and monitor all your AI models, from anywhere

Risk Management

Manage model risks, issues and mitigation actions to business standards

Regulatory Compliance

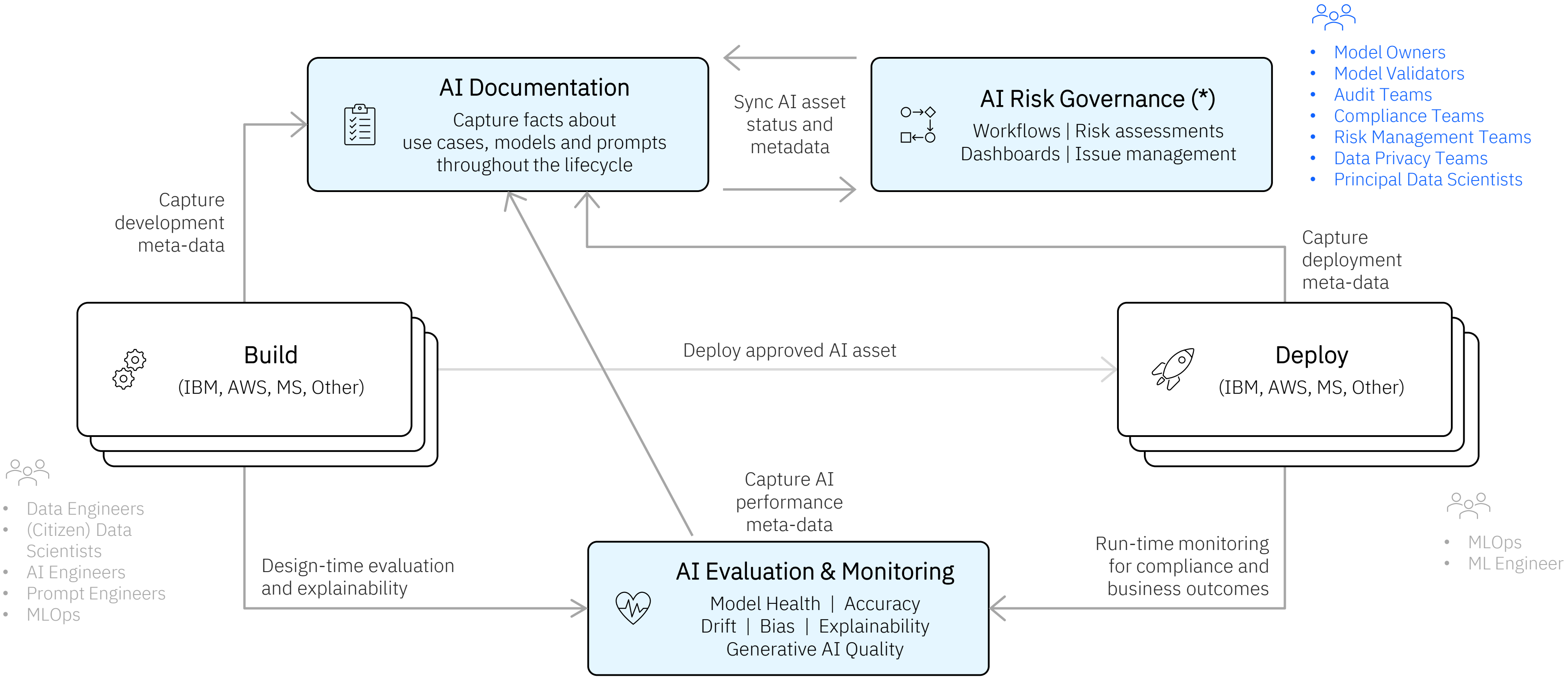
Ensure you adhere to external AI regulations for audit & compliance

Bring together all technical and non-technical stakeholders

Which is easier said than done

Common challenges		Optimization approach
AI governance collaboration requires lots of **manual work**; amplified by changes in data and model versions.	→	**Automate** the governance activities as much as possible.
Companies have AI in **multiple tools, applications and platform**, developed inside and outside the organization	→	**Consolidate** as much as possible in one governance platform.
Governance is **not a one-size-fits-all** approach.	→	**Configure** to your specific situation.
Constrain technical teams in their choice of technology.	→	**Open** architecture to wrap around tooling of choice.

watsonx.governance



AI Documentation

Capture facts about use cases, models and prompts throughout the lifecycle

Sync AI asset status and metadata

AI Risk Governance (*)

Workflows | Risk assessments
Dashboards | Issue management

- Model Owners
- Model Validators
- Audit Teams
- Compliance Teams
- Risk Management Teams
- Data Privacy Teams
- Principal Data Scientists

Capture development meta-data

Capture deployment meta-data

Build

(IBM, AWS, MS, Other)

Deploy approved AI asset

Deploy

(IBM, AWS, MS, Other)

- Data Engineers
- (Citizen) Data Scientists
- AI Engineers
- Prompt Engineers
- MLOps

Capture AI performance meta-data

Design-time evaluation and explainability

AI Evaluation & Monitoring

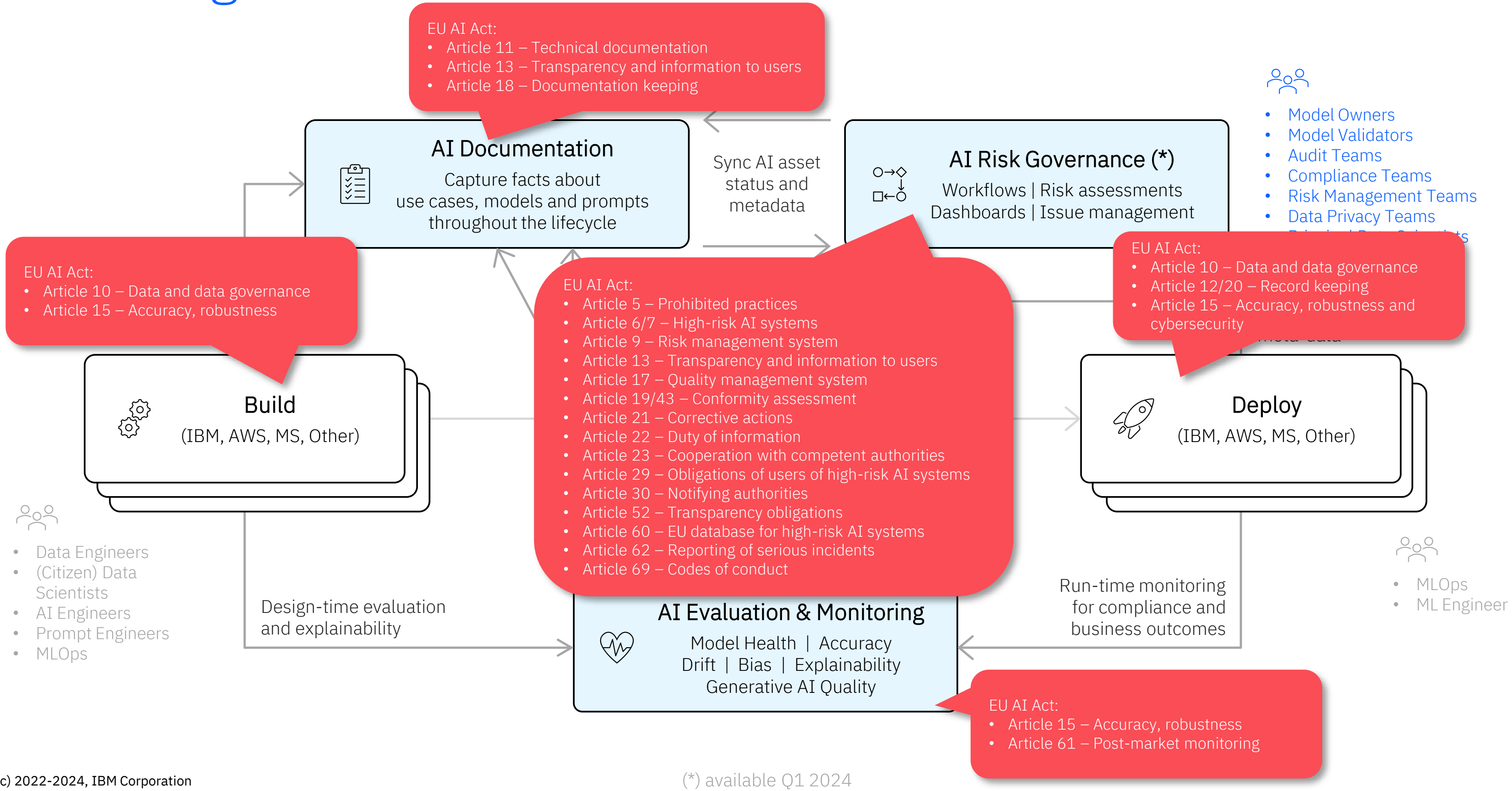
Model Health | Accuracy
Drift | Bias | Explainability
Generative AI Quality

Run-time monitoring for compliance and business outcomes

- MLOps
- ML Engineer

(*) available Q1 2024

watsonx.governance



EU AI Act:
- Article 11 – Technical documentation
- Article 13 – Transparency and information to users
- Article 18 – Documentation keeping

AI Documentation

Capture facts about use cases, models and prompts throughout the lifecycle

Sync AI asset status and metadata

AI Risk Governance (*)

Workflows | Risk assessments
Dashboards | Issue management

- Model Owners
- Model Validators
- Audit Teams
- Compliance Teams
- Risk Management Teams
- Data Privacy Teams

EU AI Act:
- Article 10 – Data and data governance
- Article 15 – Accuracy, robustness

EU AI Act:
- Article 5 – Prohibited practices
- Article 6/7 – High-risk AI systems
- Article 9 – Risk management system
- Article 13 – Transparency and information to users
- Article 17 – Quality management system
- Article 19/43 – Conformity assessment
- Article 21 – Corrective actions
- Article 22 – Duty of information
- Article 23 – Cooperation with competent authorities
- Article 29 – Obligations of users of high-risk AI systems
- Article 30 – Notifying authorities
- Article 52 – Transparency obligations
- Article 60 – EU database for high-risk AI systems
- Article 62 – Reporting of serious incidents
- Article 69 – Codes of conduct

EU AI Act:
- Article 10 – Data and data governance
- Article 12/20 – Record keeping
- Article 15 – Accuracy, robustness and cybersecurity

Build

(IBM, AWS, MS, Other)

Deploy

(IBM, AWS, MS, Other)

- Data Engineers
- (Citizen) Data Scientists
- AI Engineers
- Prompt Engineers
- MLOps

Design-time evaluation and explainability

AI Evaluation & Monitoring

Model Health | Accuracy
Drift | Bias | Explainability
Generative AI Quality

Run-time monitoring for compliance and business outcomes

- MLOps
- ML Engineer

EU AI Act:
- Article 15 – Accuracy, robustness
- Article 61 – Post-market monitoring

(*) available Q1 2024

IBM