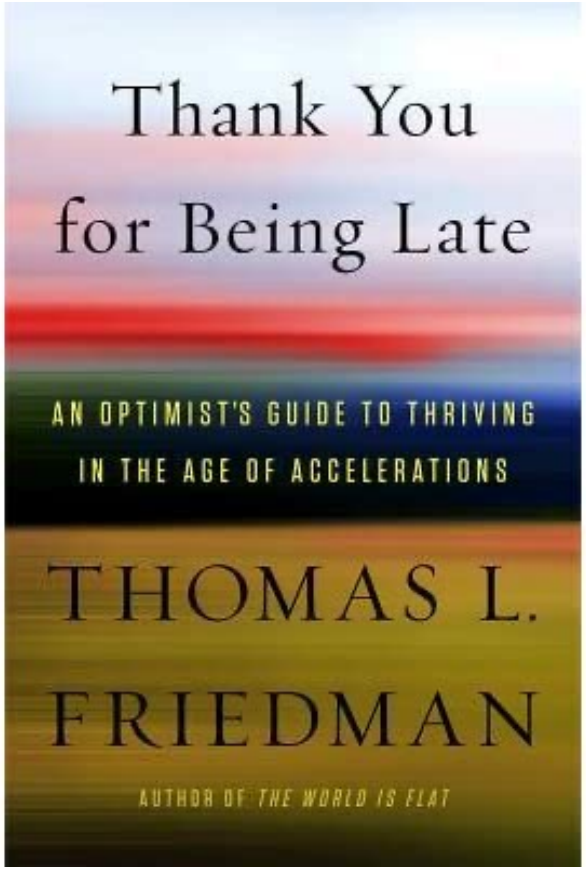
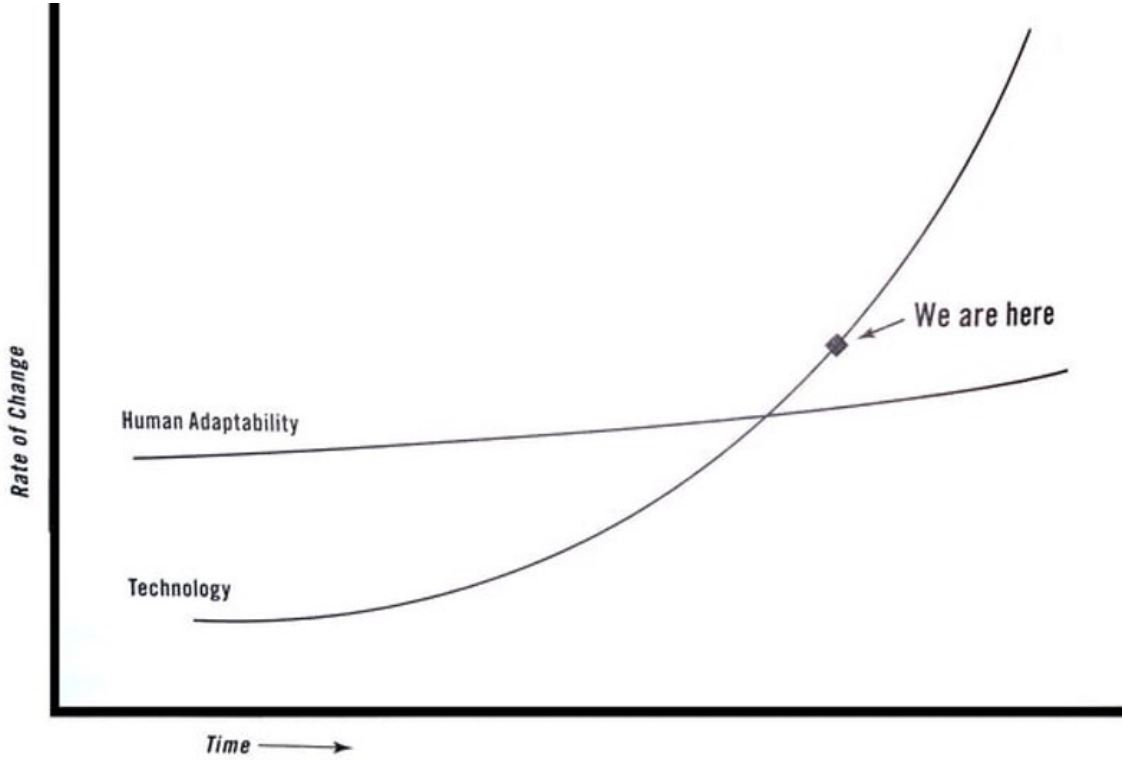
Reimagine AI Governance

Carlvin Paris
Business Unit Executive, Data Science and AI
cparis@us.ibm.com

Doug Stauber
Principal Product Manager, AI Governance
dstauber@us.ibm.com

AI Governance is essential in preventing catastrophic events that put businesses at risk


Thank You
for Being Late
AN OPTIMIST'S GUIDE TO THRIVING
IN THE AGE OF ACCELERATIONS
THOMAS L.
FRIEDMAN
AUTHOR OF THE WORLD IS FLAT


Rate of Change
We are here
Human Adaptability
Technology
Time

Responsible AI takes many dimensions

From principles to actions

AI Ethics

what should be done

principles, values, norms, laws, regulations

Trustworthy AI

how to instrument it

techniques, algorithms, software, best practices

AI Governance

how to operationalize it

mechanisms, systems, and processes to keep AI trustworthy

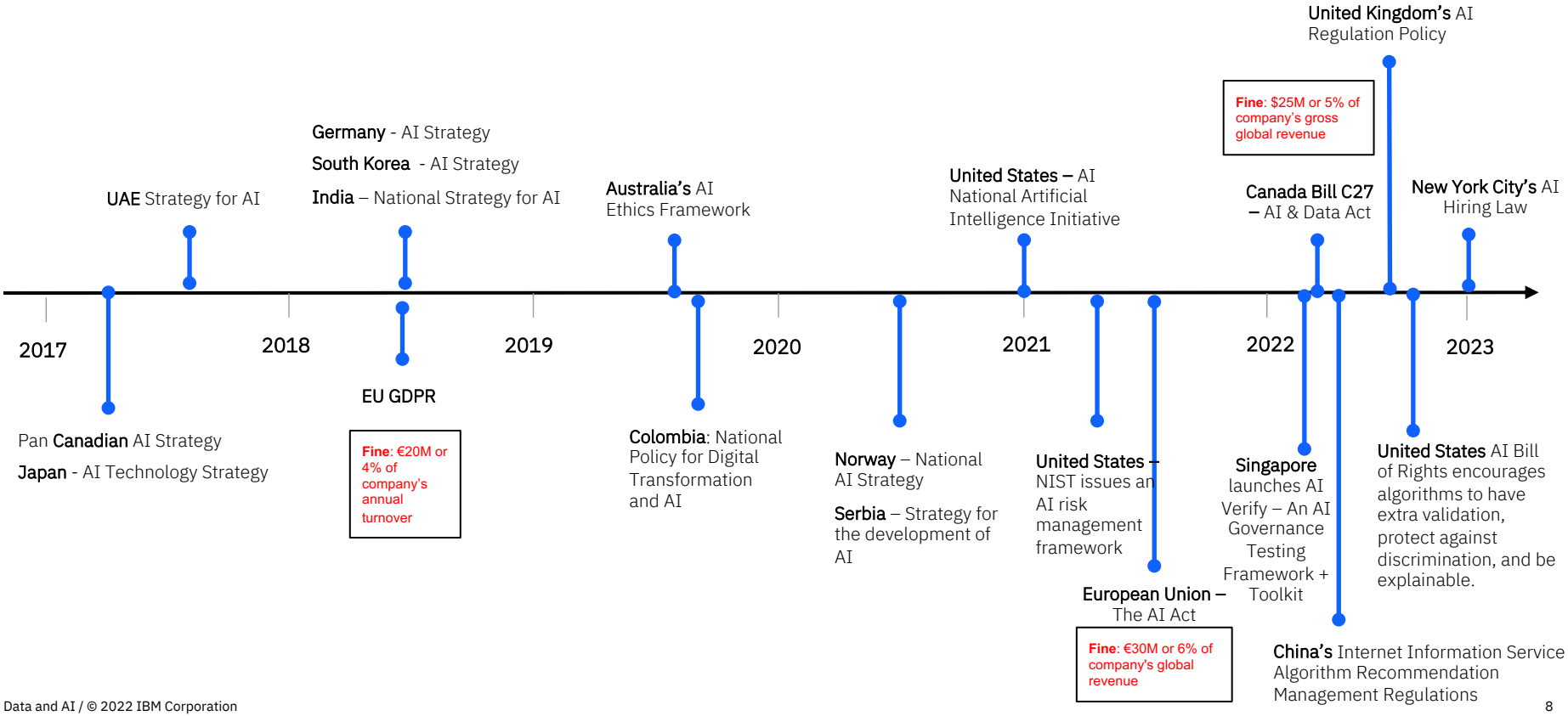
BlackBox Solution for Aviation Safety

BlackBox Solution for AI
IBM AI Governance

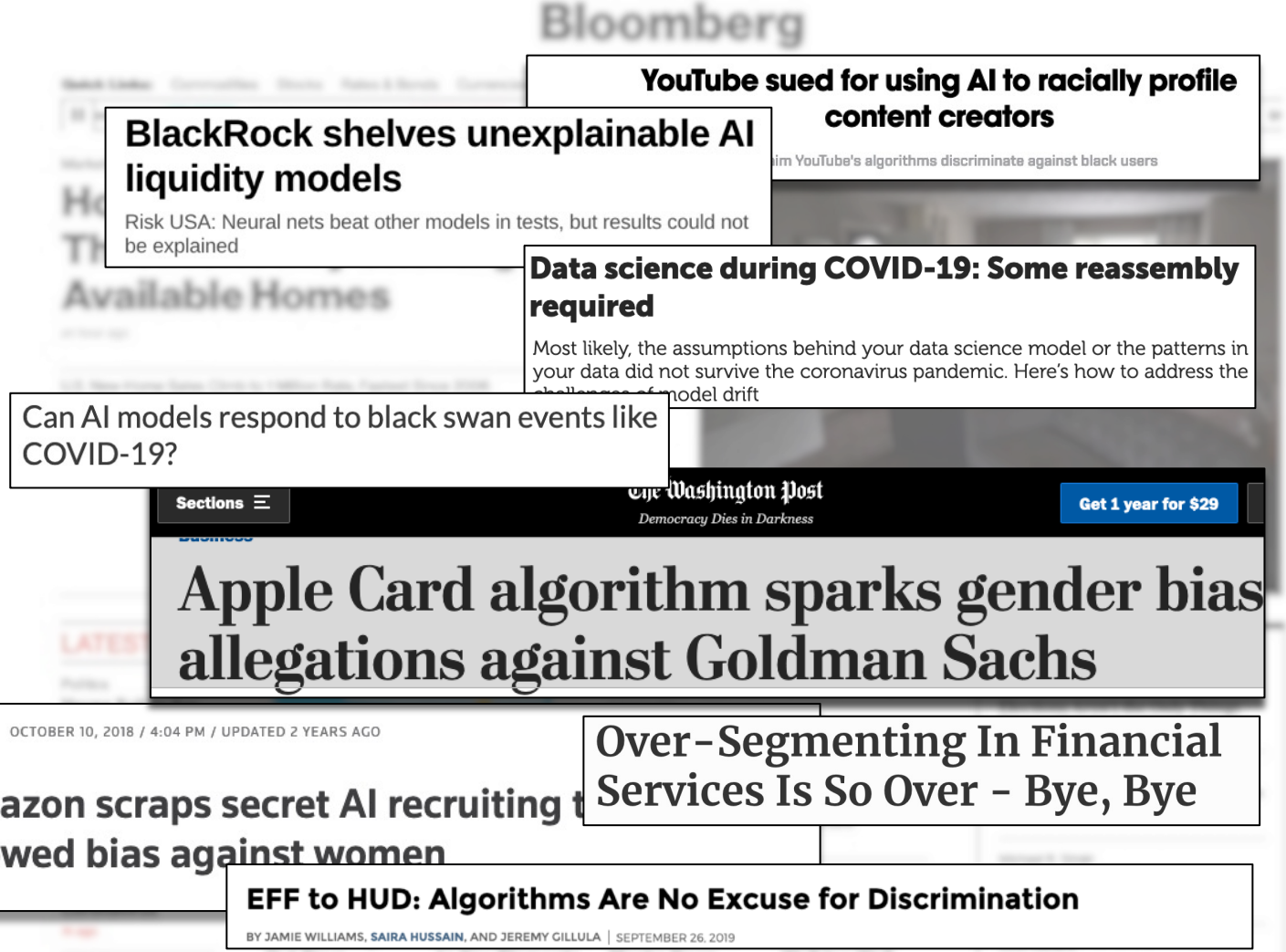
These 4 industry changes are driving a new paradigm for operationalizing AI.

1. Regulation
2. Responsible AI
3. Risk
4. Stakeholders

Regulation: AI Policies are accelerating over time



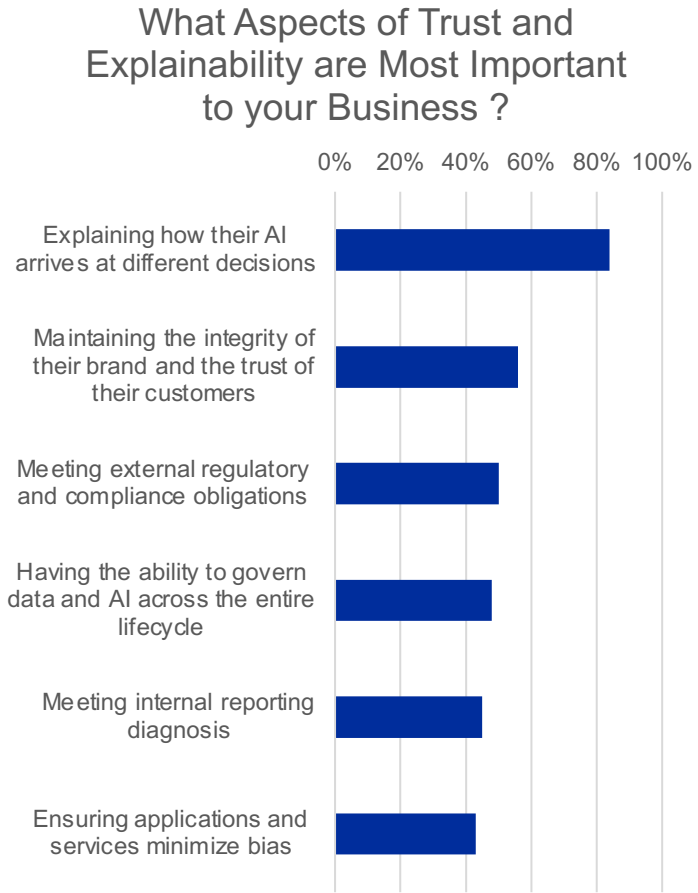
Responsible AI protects against loss of data privacy, reduced customer loyalty and trust



Risks throughout entire AI workflow

Organizations need to mitigate risks of:

- Deciding not to use certain technologies / practices
- Using personal information when needed and with user's consent
- Ensuring automated decisions are free from bias
- Customer confidence by providing explanations for business decisions
- Fraud to the organization and to customer's accounts
- Delays in putting models into production
- Inefficiency of AI lifecycle stakeholders



Source: IBM Global AI Adoption Index 2022

Stakeholders increasing beyond traditional players

Mike
Data Scientist

Understand Use Case & Feasibility

Ann
Data Engineer

Find & provide Data

Explore & understand Data

Greg
Business Analyst

Prepare & label Data

Share Insights

John
Business Lead

Extract Features

Train Models Automate Training

Experiments

Paul
Data Scientist

Deploy, Manage, Scale, Monitor in Prod

Priya
ML Engineer

Predictions for Processes or Apps

Jennifer
App Developer

Optimize via Decision Optimization

Deb
Operations Researcher

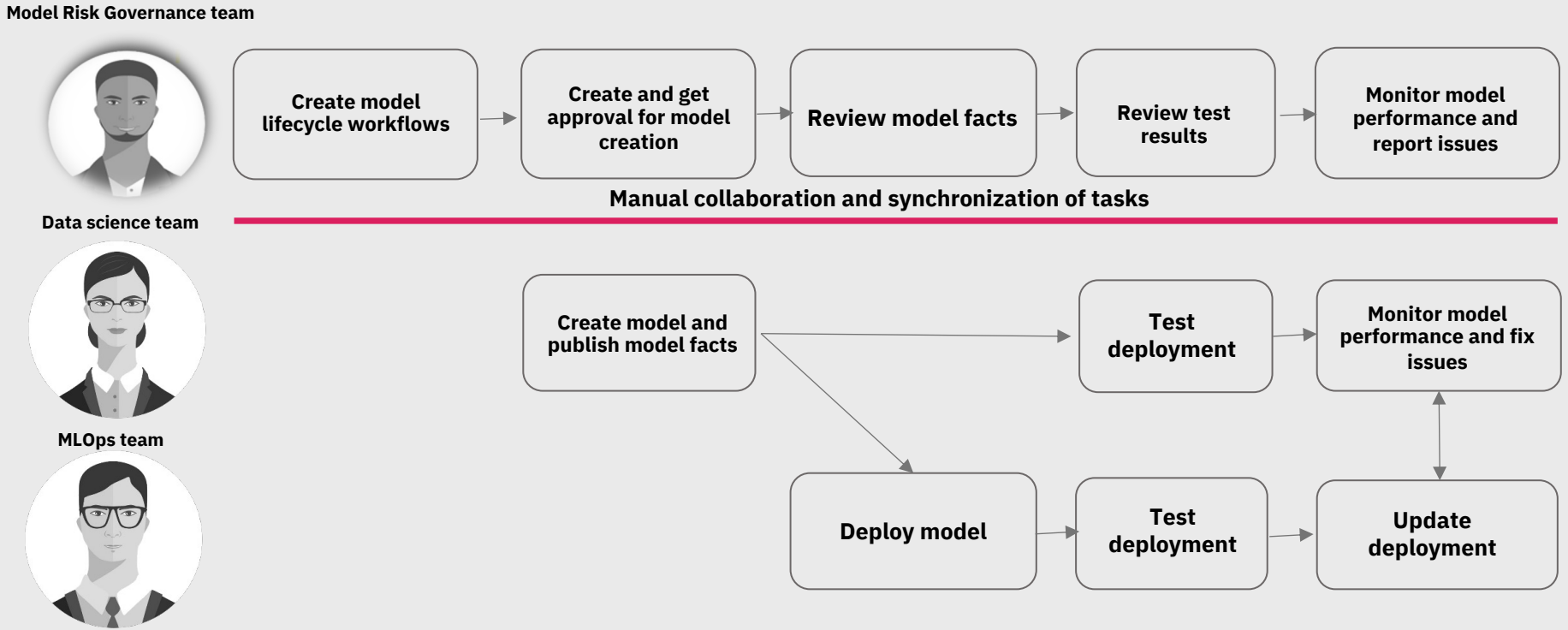
- **CIO –** Practices responsible AI
- **CFO** – Risks to profitability
- **CMO-** Risks to brand
- **CRO** – Risks to enterprise
- **CDO** – Efficient Data Operations
- **HR Lead** – Potential Job Impacts
- **CEO** – Organizational Accountability

New!

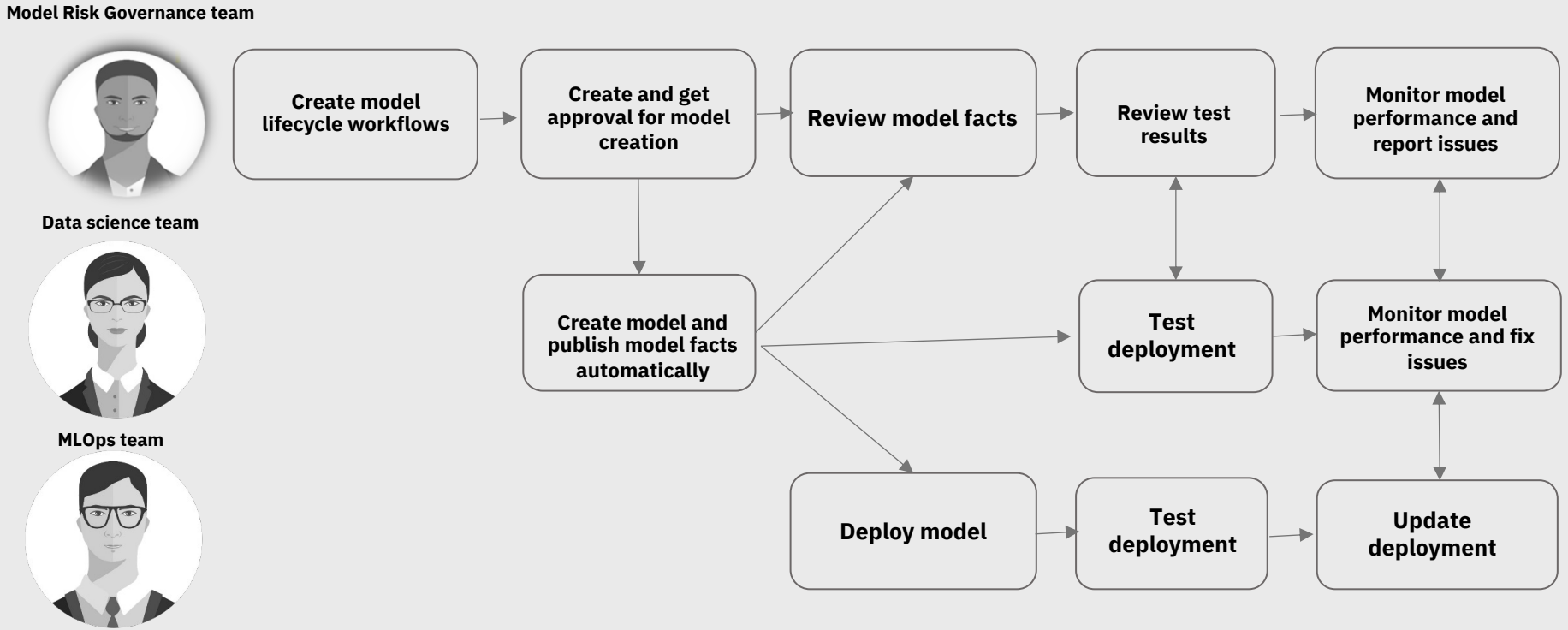
GRC Tools provide governance

Maria
Model Validator / Risk Officer

Sample AI Governance workflow: most implementations



Sample AI Governance workflow: *integration* and *automation*



Industry changes leading to Reimaged AI Governance

AI Governance	Before	After	IBM AI Governance Solution
Responsible AI	• Accuracy and model performance are rated above all else	• Equal weight for a broader set of metrics like **fairness, drift, explainability, quality**, etc.	Lifecycle Governance
Risk	• Model trust established at the end of AI Lifecycle (if at all)	• Trust established throughout… starting from **use case identification**… to ensure model robustness	Risk Management
Stakeholders	• Silo'd projects focused on collaboration between Data Science, Business leadership	• **Enterprise-wide** organization required driving C-suite discussions	
Regulations	• Limited regulations • Data scientists time spent prepping, building, and deploying models	• Newly imposed regulatory requirements • **Regulations require** them to document lineage and metadata	Regulatory Compliance

The IBM AI Governance Solution

In a world where *trust, transparency and explainable AI* matters, every organization wants the comfort and compliance of understanding how analytic insights and decisions are being made. The IBM AI Governance solution provides:

Lifecycle Governance

- Monitor, catalog, and govern AI models from anywhere, across the AI lifecycle.
- Automate the capture of model metadata for effort-less report generation
- Drive transparent, explainable AI at scale
- Increase accuracy of predictions by identifying how AI is used and where it is lagging.

Risk Management

- Automate facts & workflow management, complying to business standards.
- Identify, manage, monitor and report on risk/compliance at scale.
- Use dynamic dashboards for clear, concise customizable results
- Enhanced collaboration across multiple regions and geographies.

Regulatory Compliance

- Help adhere to external AI regulations for audit & compliance
- Translate external AI regulations into policies for automatic enforcement
- Use dynamic dashboards for compliance status across policies and regulations.

Comprehensive
Govern the **end-to-end AI lifecycle**

Open
Support governance of models built and **deployed in 3rd party tools** across multiple deployment options

Multi-persona
so it works across your entire organization

Let's get started together

End-to-End Solution for AI Governance

Proof of Value
FREE

- AI Governance Briefing
- AI Health Check
- Setup Trial Environment
- Prove AI Governance with Sample Model
- Establish Roadmap for Delivery

Software Bundle

- Lifecycle Governance
- Risk Management
- Regulatory Compliance

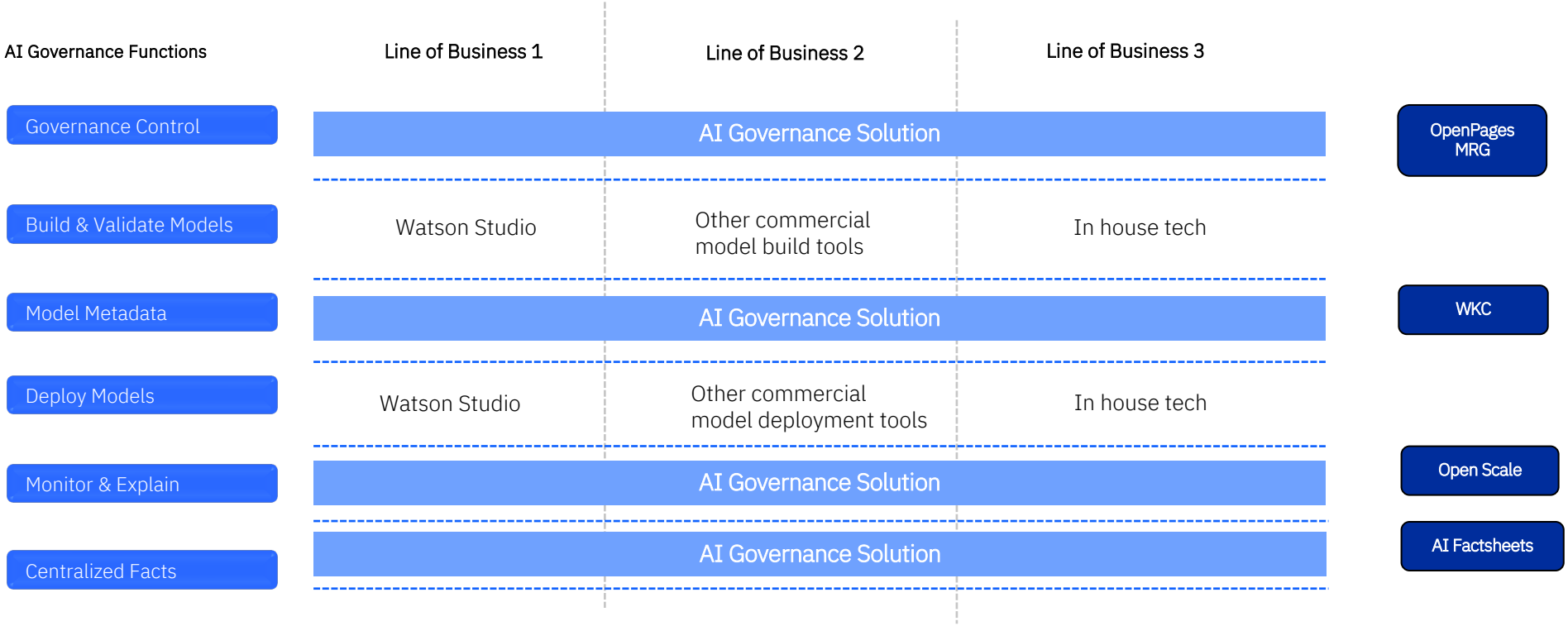
Expert Labs Services

- Installation & configuration
- Pattern assets
- Model inventory & fact collection
- Governance workflow & risk assessment
- Model monitoring & evaluation

Scenarios

Putting AI Governance to work

A typical customer context



Scenario 1:
Lifecycle Governance

Business Challenge

Data Scientists build multiple AI models before selecting a model to be sent for validation. Model Risk Management teams need additional information from the data scientist about why a specific model was selected, what parameters were used, etc., before deciding. This back and forth leads to a delay in model approval and deployment to production.

Solution

IBM AI Governance can accelerate the time to get models into production by adding:

1. Meta data collection of the models developed and deployed
2. Automatic metric data collection on models deployed
3. Providing always-up-to-date dashboards to organize views for all personas in the organization

Scenario 2:
Risk Management

Business Challenge

Monitoring of models in production is not just limited to monitoring if they are fair, have drift, etc. Models need to be used for the right use cases for which they have been approved. E.g., a model which has been approved for use for clients in CA will require a different sets of checks as compared to a model being used for clients in NY or Europe. How can organizations make sure that models undergo the right tests before being deployed and used in production?

Solution

IBMs AI Governance can provide a framework to operationalize AI with confidence by:

1. Establishing a customized workflow with the right checks and thresholds to cater to the unique needs for each region
2. Reporting of all the information and results in a standardized and comprehensive governance tool for the risk advisory team to manage.

Scenario 3:
Regulatory Compliance

Business Challenge

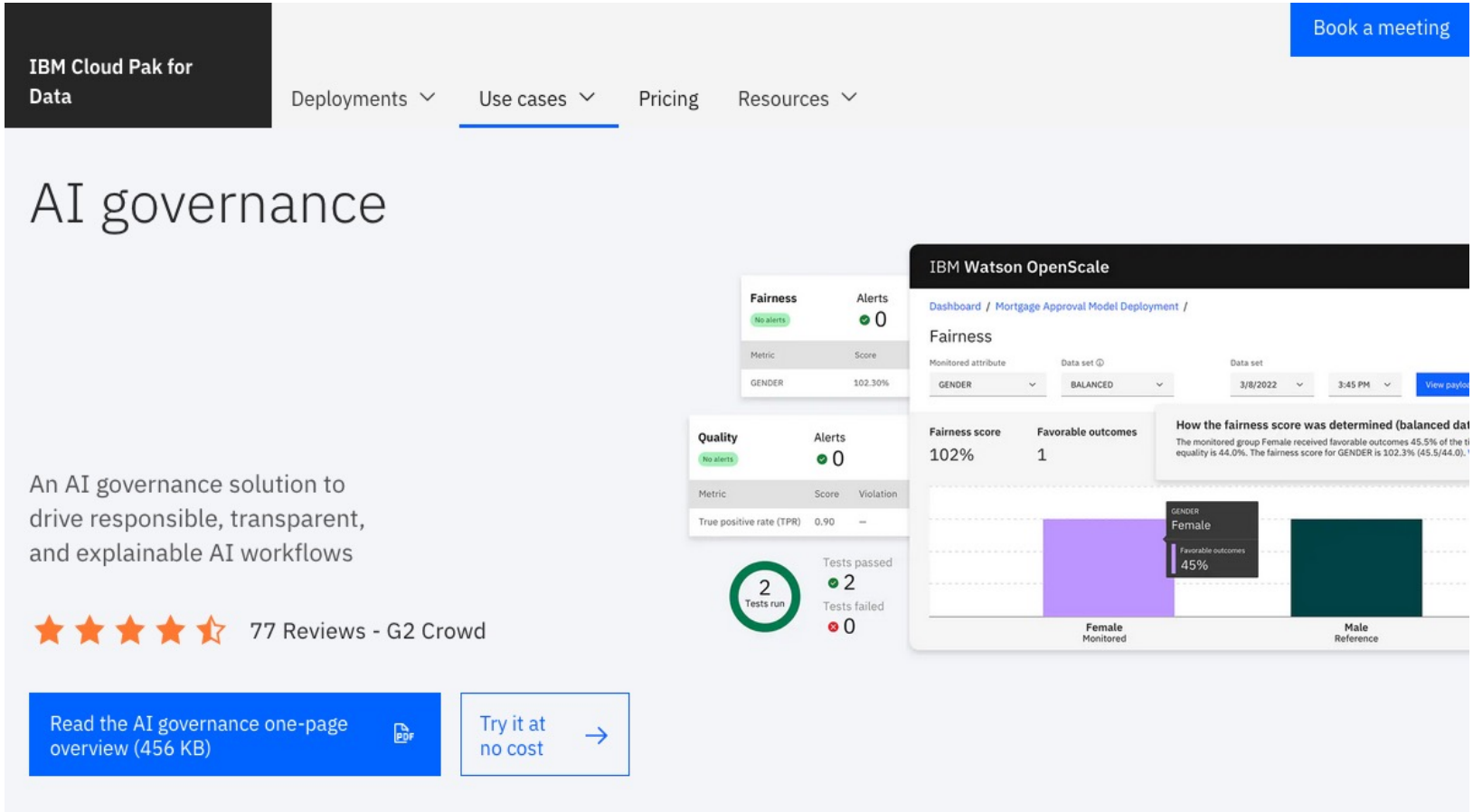
A big focus area of the new AI Regulations is that of fairness in hiring and promotion decisions. AI models which make these decisions are built without having knowledge of the gender or ethnicity of the person for whom the hiring decision is being made. However, this information can be leaked to the model from correlated features. How can organizations ensure that such models are fair?

Solution

IBM AI Governance provides state of the art technology to solve such problems by:

1. Ensure the models are fair when they are built
2. Continuously monitor models for Indirect bias where gender/ethnicity information can be leaked to the model due to correlated features
3. Recommend features on which the model is likely to exhibit bias

AI Governance is essential in preventing catastrophic events that put businesses at risk



[Visit our website to learn more, try a tutorial, or talk to an expert: https://www.ibm.com/products/cloud-pak-for-data/ai-governance](https://www.ibm.com/products/cloud-pak-for-data/ai-governance)

Questions and Answers

Thank you

IBM AI Governance Roadmap

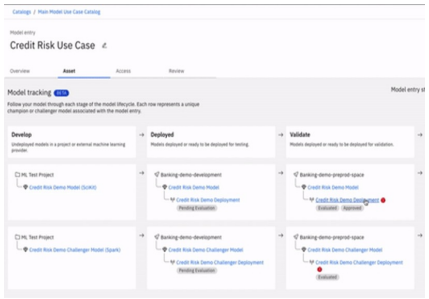
2H'2022

Model Metadata Capture

Export Factsheets to PDF/DOCX/HTML file format

Export customizable Factsheets templates

Model Entries will sync with standalone OpenPages instances



Model Monitoring

Drift 2.0 – data distribution drift, feature drift & recommendations to fix drift

Enhanced support for latest trust algorithms from IBM Research through new fairness UI and SHAP explanation support

360º view for model health including new metrics such as latency, number of records scored, and CPU usage

Compare champion and challenger models with the same payload data

1H'2023

Model Metadata Capture

Adding images and attachments to Factsheets to enhance data scientist explainability

Displaying feature transformation on Factsheet to illustrate data wrangling steps for improved transparency

Supporting Model Versioning for improved experiment tracking

Model Monitoring

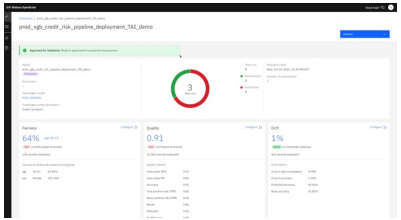
Users can perform root cause analysis for any violations they may encounter by deep-diving into the data though data slicing

Risk Workflow Orchestration

Enhanced AI Governance Dashboard with metric violation indicators and lifecycle-based charts

Support for regulatory frameworks such as Responsible AI Institute's (RAII) framework

New workflow artifacts will enable governance of model features, ensemble models and unauthorized usage of models



Gartner Forecasts Worldwide Artificial Intelligence Software Market to Reach

$62 Billion

in 2022[1]

Gartner predicts that 30% of IT organizations that fail to adopt AI will no longer be operationally viable by 2022.[3]