IBM India/South Asia Blog

How to build AI you can trust, explain, and responsibly operationalize?

Apr 15, 2024

By Geeta Gurnani

It is encouraging to see that leading global organizations today are increasingly acknowledging responsible AI as the way forward. However, despite good intentions, evolving technologies, and the advantage of resources, achieving responsible AI can be quite daunting for businesses.

Earlier, I shared my views on the what and why of responsible AI adoption, underscoring the significance and role of governance in helping Indian businesses adopt responsible AI. In this blogpost, I shall outline the hurdles your business may encounter in this journey and the key steps that your business can take to operationalize responsible AI successfully.

AI-Related Risks to Consider

Acknowledging the use of responsible AI is just the first step - implementing this comes with its unique set of challenges your business must tackle. While risk in AI models can come from many sources and newer concerns are rising with the advent of GenAI, there are broadly three categories of risks your business should consider.

1. **Regulatory risks** as AI legislation is steadily progressing in many parts of the world and non-compliance can result in huge penalties for businesses.
2. **Reputational risks** as any unfavourable outcomes from AI deployments can significantly hamper your brand's perception in the public domain.
3. **Operational risks** considering that an AI project may not even make it to production, robbing your organization of the potential benefits of the solution.

In addition to assessing the above risks, skilling your workforce will be crucial in this journey. Employees need to be provided with the relevant skills to work with AI and ensure a robust AI governance framework.

AI Governance Holds the Key

To mitigate the abovementioned risks and challenges, your business needs to prioritize AI governance as an enabler for responsible AI adoption. Like any other technology, AI needs governance - the ability to direct, manage, and monitor the AI activities of your organization. Implementing AI governance can provide your business with a level of organizational rigor and human oversight of how AI models are created and deployed.

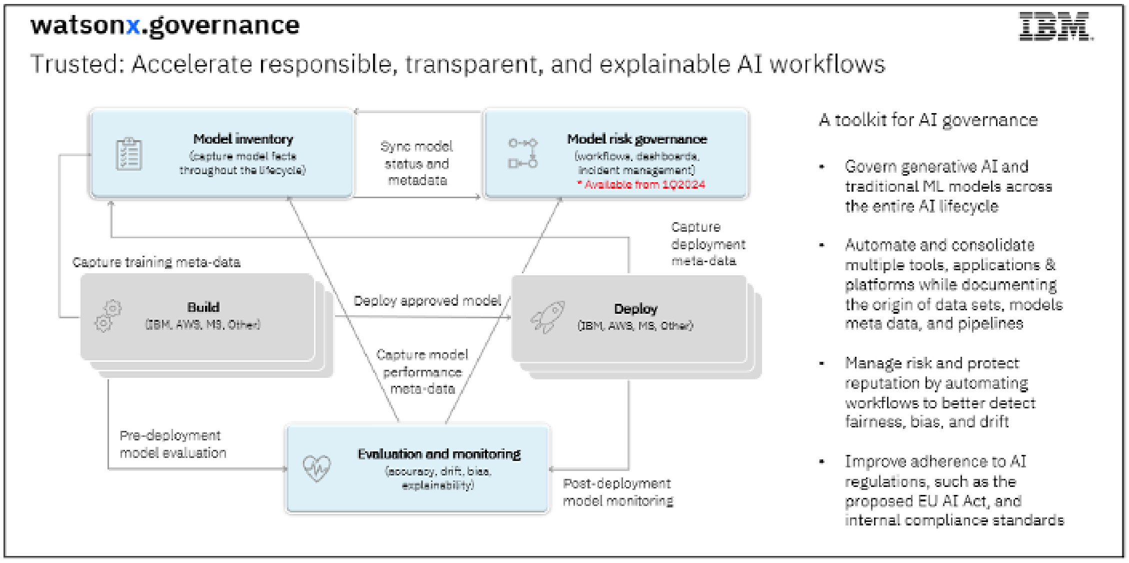
Your business needs three critical capabilities for a proper AI governance solution.

- **Monitor and evaluate models throughout their lifecycle**: Businesses using AI must be able to configure monitoring thresholds to show that they meet required regulatory standards for model performance, as well as ensure that no personal identifiable information (PII) is leaking from the model and may even have to be able to explain model output.
- **Track relevant facts and metrics associated with models:** This refers to the ability to automatically gather model metrics and metadata.
- **Lifecycle and risk management**: From the initial request through the development, test, and deployment phases, the entire lifecycle process should be as automated as possible to reduce both the possibility of human error and the time to produce tangible business value. At each step of the way, the stakeholders involved need access to the right information to decide whether the model is acceptable and should be approved, or needs further development, documentation, and testing.

AI Governance Simplified with IBM watsonx.governance

Taking into account the above challenges and requirements in AI governance, IBM watsonx.governance was built to direct, manage and monitor the artificial intelligence (AI) activities of your organization by using IBM watsonx, one integrated platform, which can be deployed on cloud or on-premises. By employing software automation, this solution helps strengthen your ability to meet regulatory requirements and address ethical concerns (without the excessive costs of switching from your current data science platform).

Spanning the entire AI lifecycle, the watsonx.governance solution monitors and manages model building, deploying, monitoring, and centralizing facts for AI transparency and explainability as shown in the image below.



watsonx.governance

Trusted: Accelerate responsible, transparent, and explainable AI workflows

Model inventory
(capture model facts throughout the lifecycle)

Sync model status and metadata

Model risk governance
(workflows, dashboards, incident management)
* Available from 1Q2024

Capture training meta-data

Capture deployment meta-data

Build
(IBM, AWS, MS, Other)

Deploy approved model

Deploy
(IBM, AWS, MS, Other)

Capture model performance meta-data

Pre-deployment model evaluation

Evaluation and monitoring
(accuracy, drift, bias, explainability)

Post-deployment model monitoring

A toolkit for AI governance

- Govern generative AI and traditional ML models across the entire AI lifecycle
- Automate and consolidate multiple tools, applications & platforms while documenting the origin of data sets, models meta data, and pipelines
- Manage risk and protect reputation by automating workflows to better detect fairness, bias, and drift
- Improve adherence to AI regulations, such as the proposed EU AI Act, and internal compliance standards

To learn how you can build a robust AI governance program with IBM watsonx.governance, request a demo from our team of experts.

Geeta Gurnani is IBM Technology CTO & Technical Sales Leader, India & South Asia

Blog Categories