ModelOps:

The Path to Operationalizing AI in the Public Sector

MeriTalk
Improving the Outcomes of Government IT

maximus

Every generation has transformational technology. From the assembly line to personal computing to the cloud, these innovations have changed how people live and work. The next technological revolution is happening now with artificial intelligence (AI).

Federal agencies are currently applying AI to a variety of missions including streamlining interactions with citizens, improving fraud detection, performing predictive modeling of hurricane intensity, and rapidly identifying potential health threats to facilitate more rapid notifications and communication.

The Consolidated Appropriations Act of 2023 outlines that agencies have allocated more than $1 billion to AI research and development. Despite these investments, as agencies prepare to expand their use of the technology and build more AI models and algorithms to support their missions, many are finding it difficult to move AI projects out of pilots and into enterprise operations.

Rethink Traditional Software Development for AI Success

Many IT teams approach AI model development the same way they develop and deploy software: in a linear process that moves from development to testing and then to deployment followed by upgrades. However, this traditional software development architecture does not support the intricacies of building and deploying AI models.

AI works best when it runs on a continuous-loop development cycle. The model is designed, tested, and deployed when it shows good performance in the lab. It is then monitored while processing real data. If metrics fall below acceptable thresholds or if the model needs to be fine-tuned, it's then tested and deployed again. This process enables continuous evaluation and update cycles, which maintains the trustworthiness of the AI solution. Yet this paradigm shift from traditional software development and processes can be challenging for many agencies, requiring government leaders to rethink their processes to build and deploy AI at scale.

Accelerate AI With ModelOps Guiding Principles and Practices

Our experience in working with agencies to shift their software development practices leverages new AI/ML model operations, or "ModelOps." ModelOps offers guiding principles and practices to help agencies build an AI model development and deployment architecture that guides automated, responsible AI development and implementation. Our ModelOps approach supports the full AI model lifecycle, ensuring AI projects can move from pilot to operations at scale.

Build Your AI Model Pipeline

The key elements of ModelOps are:

- **Governance:** This element encompasses the standards, controls, and processes that are followed throughout the model lifecycle and tracks how and where models and data are used. Governance practices also address common concerns about AI, such as its trustworthiness and how it will be used, to ensure models stay in compliance with established standards.
- **Deployment:** With a goal of moving and sustaining AI models into enterprise operations, ModelOps offers a roadmap for taking models from the lab into production and scaling them across an organization. It ensures interoperability so anyone who needs to use the model can do so.
- **Monitoring:** ModelOps builds in monitoring, so IT teams know how their models are performing at all times. This helps teams identify model drift issues, in which accuracy begins to degrade due to differences between production and training data. Monitoring flags models for retraining when needed based on specified metrics – a critical step to maintain predictive accuracy.

With the overarching principles and practices of ModelOps in place, agencies can build a factory-like development process with an environment and workflows specific to AI – known as an AI model pipeline – that provides a rapid and measurable return on their IT software investment.

It is important to note that while this process has specific steps, those steps operate in a development loop, enabling later stages of the process to return to earlier steps as monitoring and testing dictate needs for additional model training on new data from live environments.

The ModelOps Process

Step 1: Build the dataset pipeline by identifying the source data, implementing any necessary data transformations, and determining how the data will be integrated.

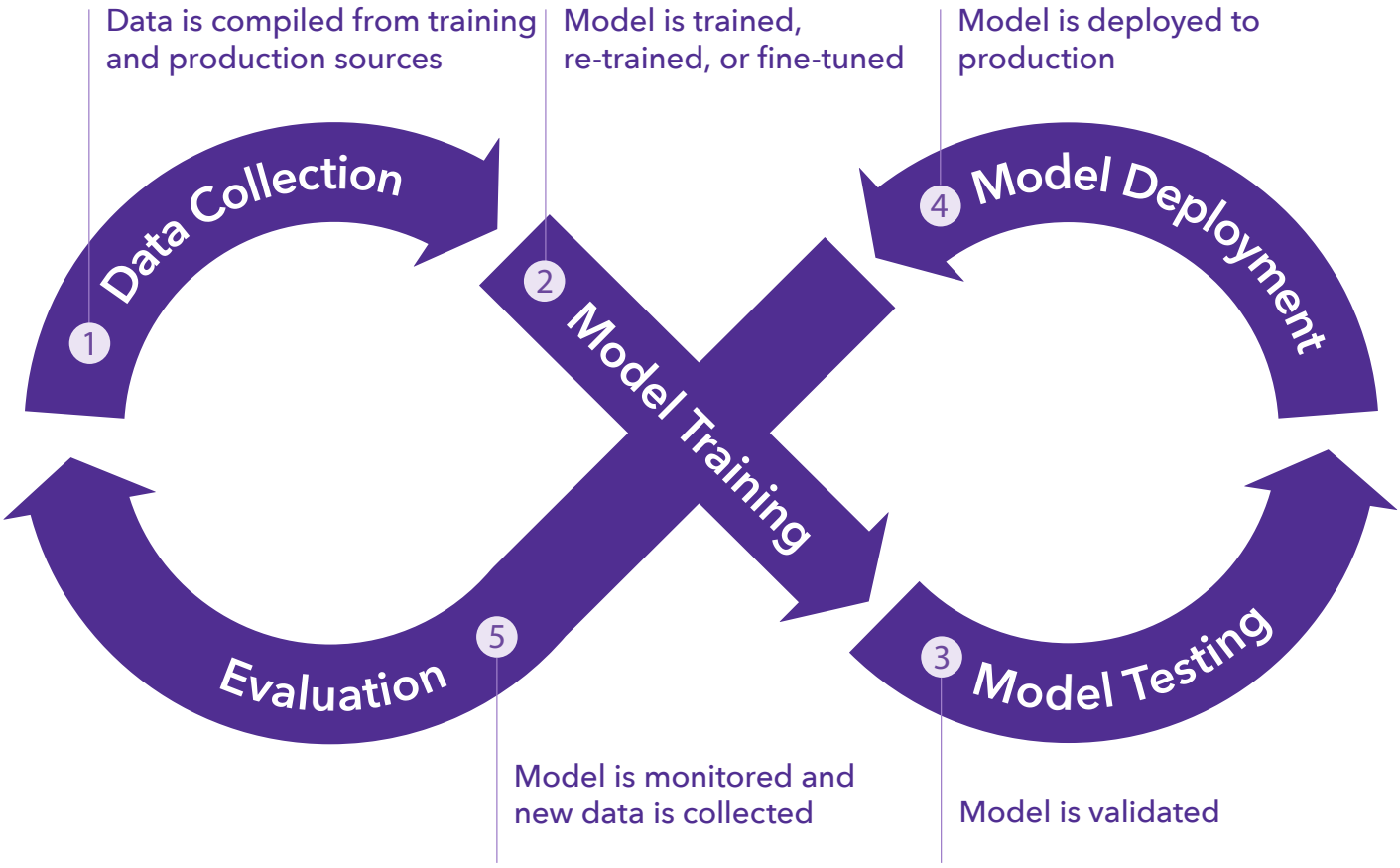
Step 2: Create or import models (from commercial entities, other government agencies, academia, or research labs) in a development environment and test those models against recent and relevant datasets.

Step 3: Move the models into a pre-production environment that provides the ability to test against and monitor live data – an essential step in preparing AI for the enterprise environment.

Steps 2 and 3 are a development loop. Models are iteratively developed as changes to inputs or model parameters are captured and incorporated for testing, verification, monitoring. Models should continue getting the input of new data in live environments.

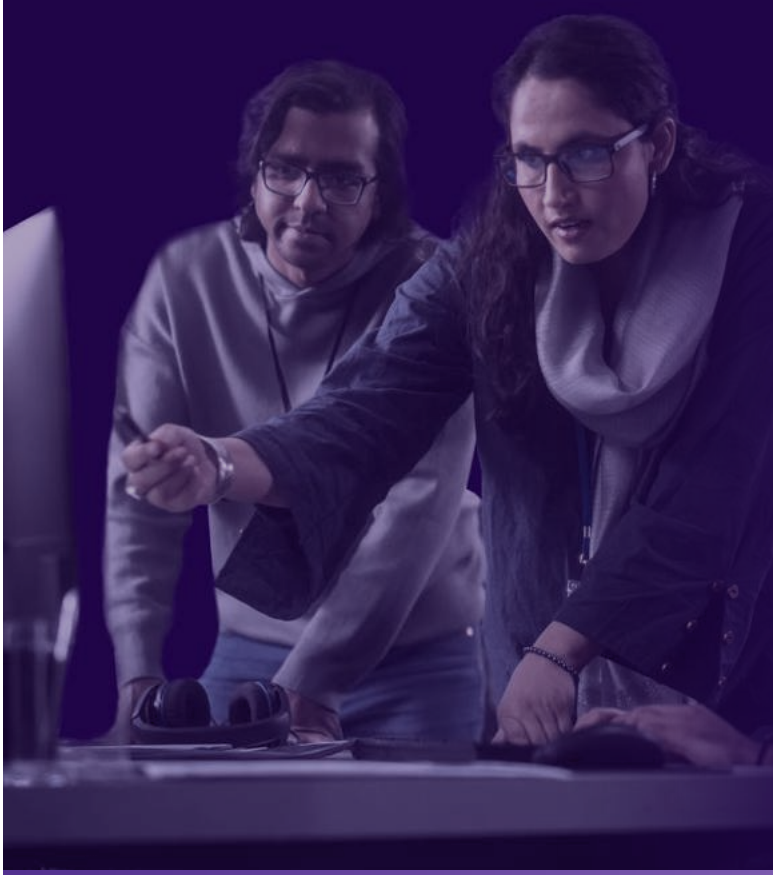
Step 4: Push models into production, returning to previous steps as needed.

Step 5: Leverage monitoring and model management protocols to flag models for updates or retraining if AI performance/accuracy begins to degrade.



Enable Better Outcomes with ModelOps

An effective implementation of ModelOps best practices and proven methodologies will be critical to how agencies responsibly operationalize AI at scale to maximize that impact, delivering high-performance outcomes and exceptional user experiences.



Benefits of the ModelOps Approach

Improve efficiency
Consistent model development and automated processes enable agencies to efficiently move AI models into production at scale to improve mission outcomes.

Boost model performance
Processes for model monitoring help to ensure expected AI performance and build trust in AI.

Mitigate risk
Built-in guardrails help agencies ensure consistency in model development and performance while bolstering security.

Increase model accuracy
AI/ML model tracking enables agencies to confirm that models do not move away from their mission efficacy by monitoring how and where their models are being used.

Reduce costs
Model re-use enables agencies to utilize whole libraries of models, including large-language models, developed by and for the government, avoiding unnecessary duplication for cost efficiency.

Enhance security
Built-in security practices safeguard AI models and agency data from misuse, helping to reduce security incidents.

Learn how Maximus can help integrate AI across your federal government enterprise at maximus.com/ai-advanced-analytics.

MeriTalk
Improving the Outcomes of Government IT

maximus