WORKSHOP 4
The Path to GenAi: From Data to Intelligence

Clare Bornstein

Advanced Analytics Platform Lead
Global Manufacturing & Supply
Takeda

Nishant Sinha

Director AI and Automation
Deloitte Switzerland

Susan Tillmann

Head Data, Analytics and
Digital Global Manufacturing & Supply
Takeda

Deloitte.

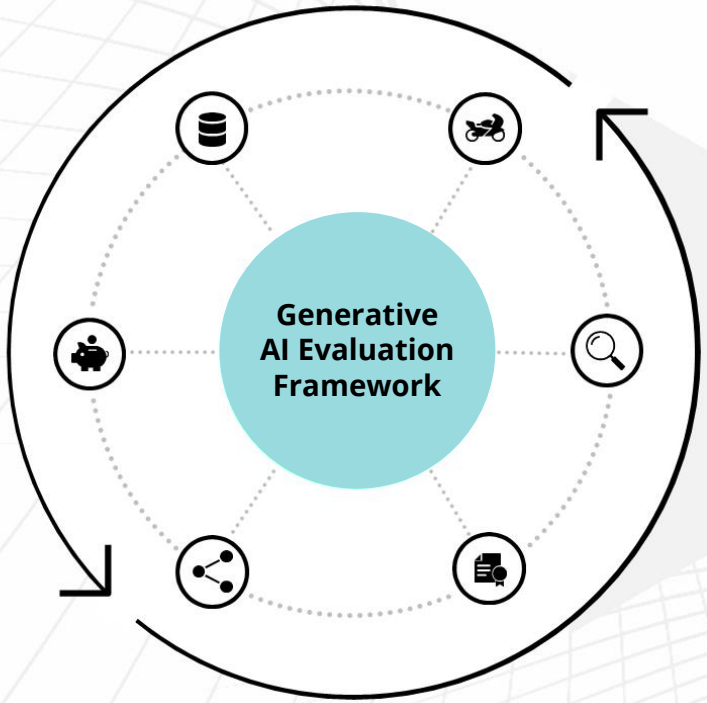
The Path to GenAi: From Data to Intelligence

Nishant Sinha
Director AI and Automation
Susan Tillmann
Head Data, Analytics and Digital, Global Manufacturing & Supply Takeda
Clare Bornstein
Advanced Analytics Platform Lead
Global Manufacturing & Supply Takeda

September 2023

INTELLIGENT HEALTH 2023

Deloitte Feasibility and Risk Framework for GenAI



Dimension	Evaluation Factor	Considerations
ABILITY TO EXECUTE	**Data Availability & Quality**	✓ Are large volumes of clean data available that can be utilized as samples for GenAI training? ✓ Is a high diversity of data available to mitigate bias potential? ✓ How difficult is it to obtain and access data?
	Process Standardization & Governance	✓ Are the target processes well documented? ✓ Do the target processes contain known "accurate" and "inaccurate" outcomes that can be used to evaluate the GenAI model's performance?
	Nature of Input Prompts & Expected Outputs	✓ How frequent and complex are the outputs of the GenAI model? (e.g., 20-page documents vs. bullet points) ✓ Will system integrations be required to facilitate data inputs or outputs interpretations?
	Change Management	✓ Is the usability of GenAI embedded in the e2e process- and application landscaope providing a seamless user experience? ✓ Is the impact of workload and –content to the employees and the organization known and well managed to avoid lack of adoption?
DEGREE OF RISK	**Bias**	✓ Is my data over/under representative of a population cohort, region, gender, demographic group? ✓ Can steps be taken to mitigate bias during training? Are there any metrics that will be used to track bias? ✓ What level of impact criticality a biased output would have on the end user?
	Ethical Use	✓ Is an appropriate process in place ensuring that the model does not tread across lines of plagiarism and copyright violations? ✓ Will the solution be subject to independent oversight and review ensuring responsibility?
	Hallucination	✓ Is there a possibility to assess and validate attributions to the source information? ✓ Is an appropriate governance model in place to ensure the "human-in the loop"? (e.g., workforce upskilling, structured oversight, ubiquitous documentation)
	Cybersecurity	✓ Have the risks for data exfiltration, Data/Model poisoning, model stealing and adversial attacks being addressed? ✓ Is there a security architecture in place that addresses the key areas of security control Infrastructure and Network, Access Management, Monitoring and Data Protection?
	IP Protection	✓ Will information be shared with third parties through prompt engineering resulting to potential data leakage?
	Patient Health and Safety	✓ Is the model capable to process and provide medical information in prescience manner to avoid mistakes which can lead to adverse consequences to human health? ✓ Can the model consider appropriate emotional tone in the conversation to account for individual health status and ability to understand information?

The Path to GenAi: From Data to Intelligence

Clare Bornstein
Global Manufacturing and Supply: Data, Analytics & Digital

September 2023

Better Health, Brighter Future

A closer look at Generative AI…

All applications of AI, whether a generative algorithm or a traditional machine learning model, produce outputs based on the inputs they are trained on. OpenAI's GPT-4 and GPT-3.5 models have made headlines in recent months for their widespread success; but what data have these models learned from?

ChatGPT+: GPT-4

Developer: OpenAI
Model Released: March 14, 2023
License: Proprietary
Training Set: Undisclosed, proprietary

ChatGPT: GPT-3.5

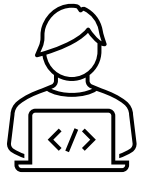
Developer: OpenAI
Model Released: November 30, 2022
License: Proprietary
Training Set: Undisclosed, proprietary

GPT-2

Developer: OpenAI
Released: February 14, 2019
License: MIT (Open Source)
Training Set: BookCorpus & WebText (Open Source)

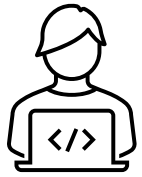
All of these OpenAI models are considered general knowledge; their outputs are limited by the relationships they have been taught during training.

A model is only as good as the data it is trained on.



Hey ChatGPT, can you tell me what tyres are made of?

Hello! Tyres are typically made of several layers of rubber, including natural rubber, synthetic rubber, and other materials such as carbon black, silica, and various chemicals.

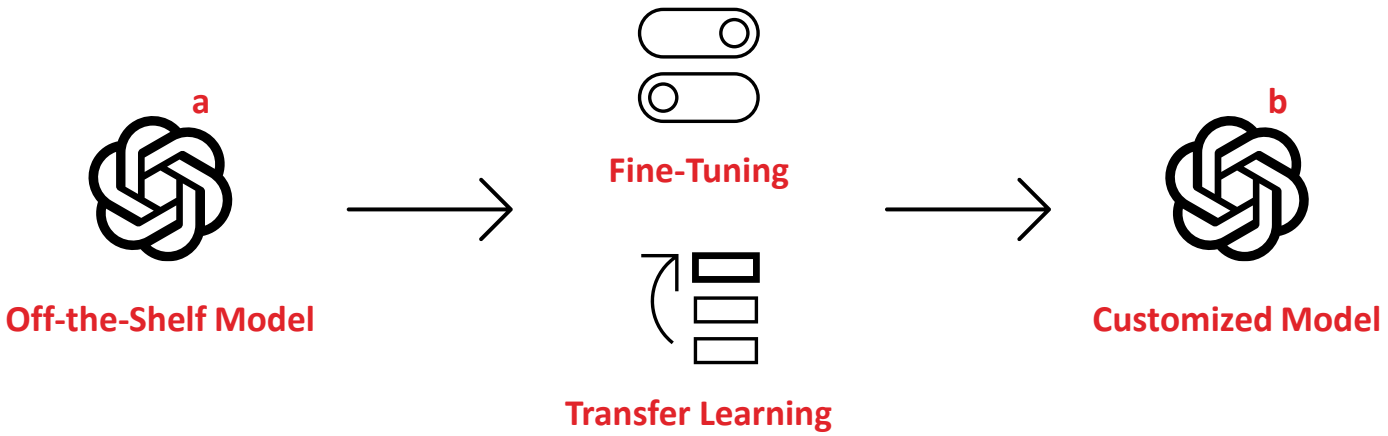


Hey ChatGPT, can you tell me the production yield of Pirelli C3 tyres produced in the EU over the past 3 months?

I'm sorry, but as an AI language model, I do not have access to up-to-date information on Pirelli’s manufacturing plans for its tyres.

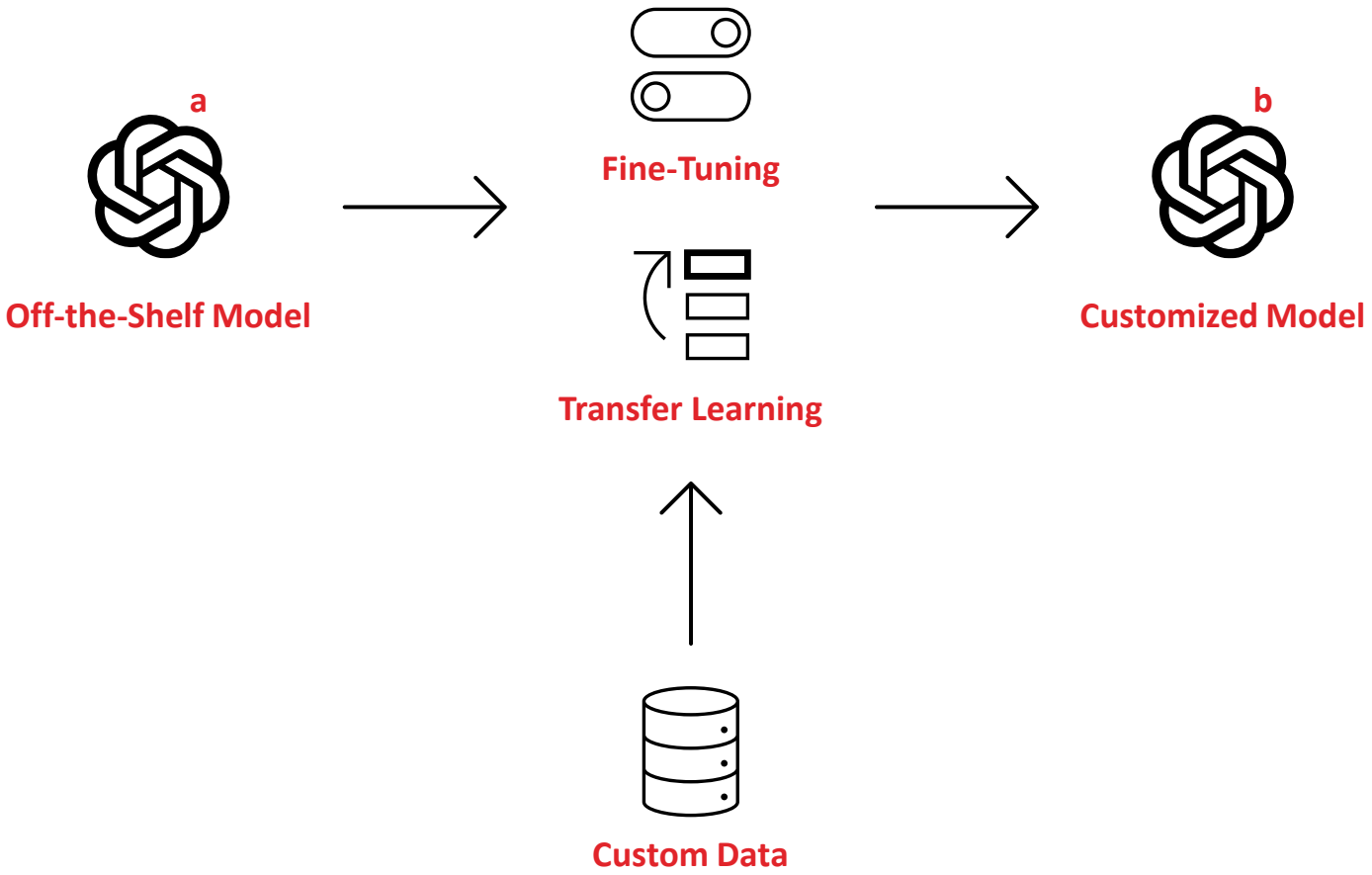
Can we customize?

With a skilled data scientist, we can improve many off-the-shelf models, or any model for that matter, by enriching them through fine-tuning and transfer learning.



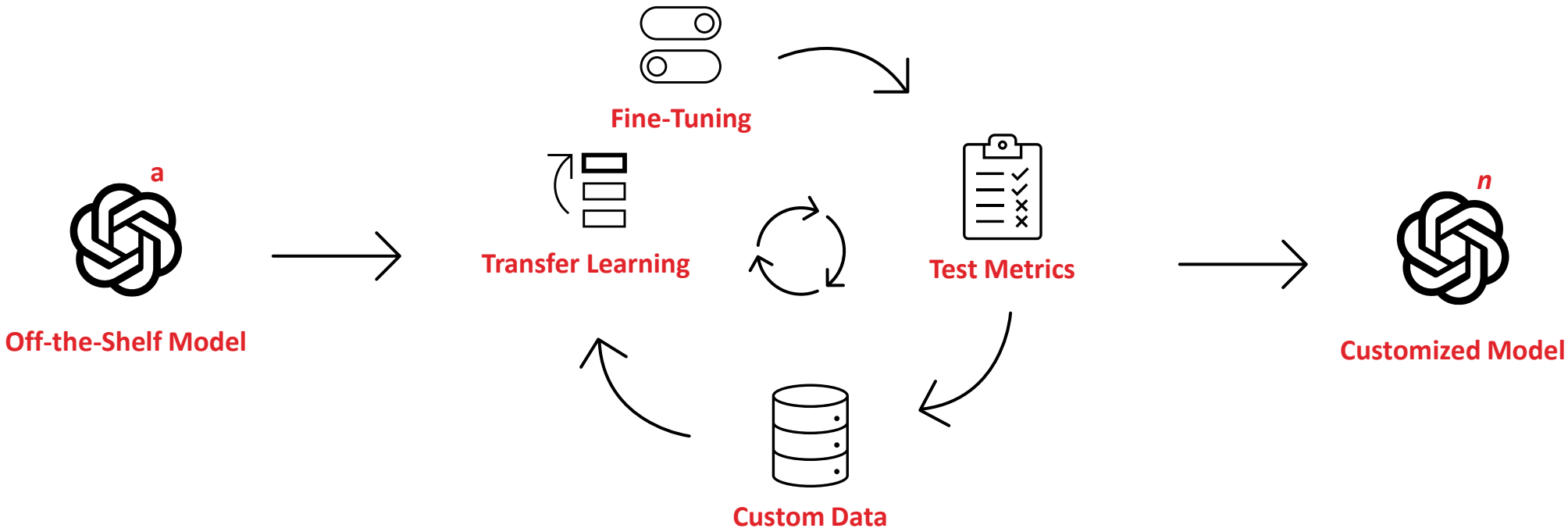
What are we customizing with?

The objective of enrichment is to teach a model about information that it hasn't seen in its original training. To make models suitable for a specific purpose, we need to supply our enrichment methodology with high quality data that is relevant for the model's application.



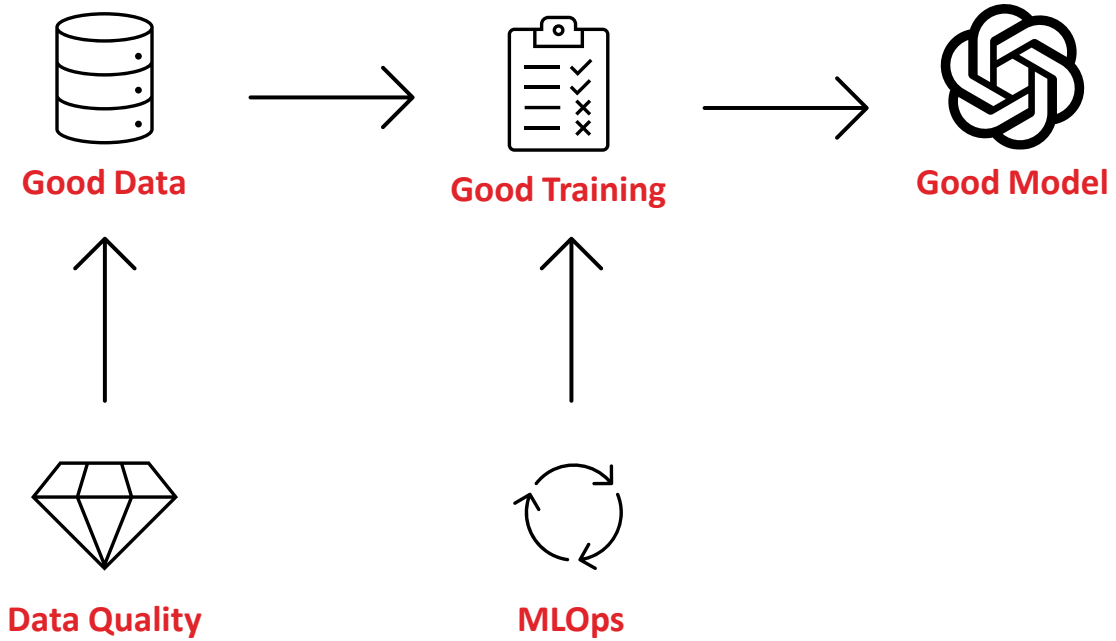
What if we could continuously customize?

To maintain relevance, many models must periodically retrain on new information. We can automate the process of feeding new data to the training cycle. Further, we can use model metrics to test the quality of models built by our automation, and decide which to automatically promote for use.



The big picture…

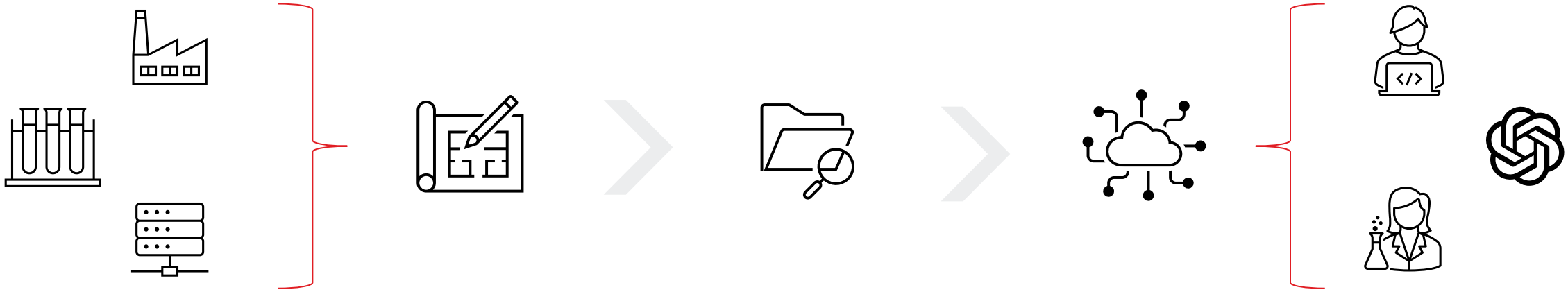
In short, to create a good quality model that is continuously fit for purpose, an organization must have two things: relevant data, and a means of ensuring the model can learn from it. We accomplish this through two principles: data quality, and machine learning operations.



Data is only as good as our ability to find, interpret, and utilize it.

Data Quality: Foundations for a robust model

Feeding our model with quality data is essential for producing a relevant model. Although many organizations have plenty of data, it must be curated it in a way that a model can learn from it.



Collecting relevant data from source

Structuring and contextualizing data to optimize **utilization**

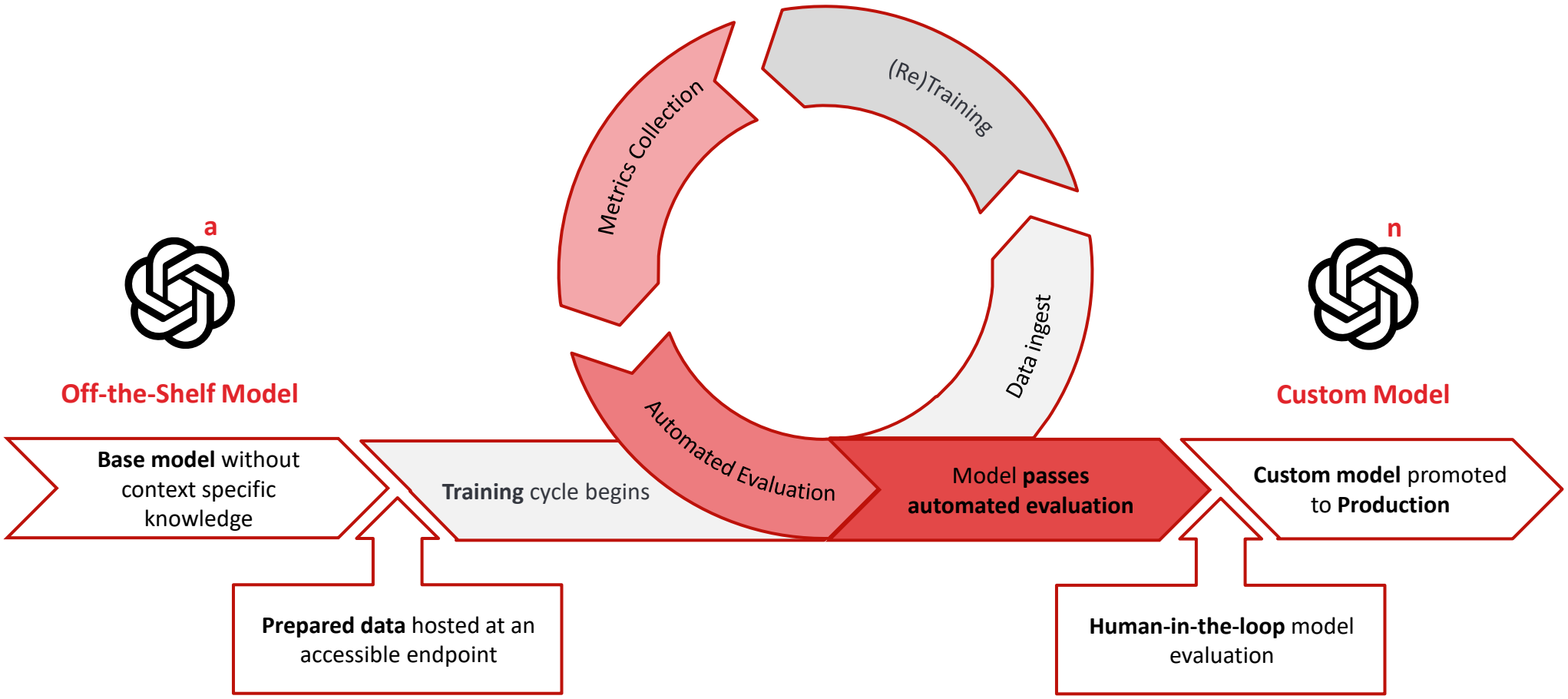
Cataloguing data to ensure it is **findable**

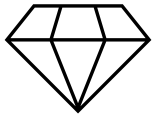
Hosting data such that it is **accessible** from multiple contexts

Consumption of data in ad-hoc or automated analysis

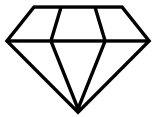
MLOps: Keeping our model relevant

Machine Learning Operations, or MLOps, is the process of automating the training, testing and deployment of a machine learning model. This process enables a given model to continuously update its knowledge base with new context-based data, and ensure long-term relevance.





A model is only as good as the data it is trained on.

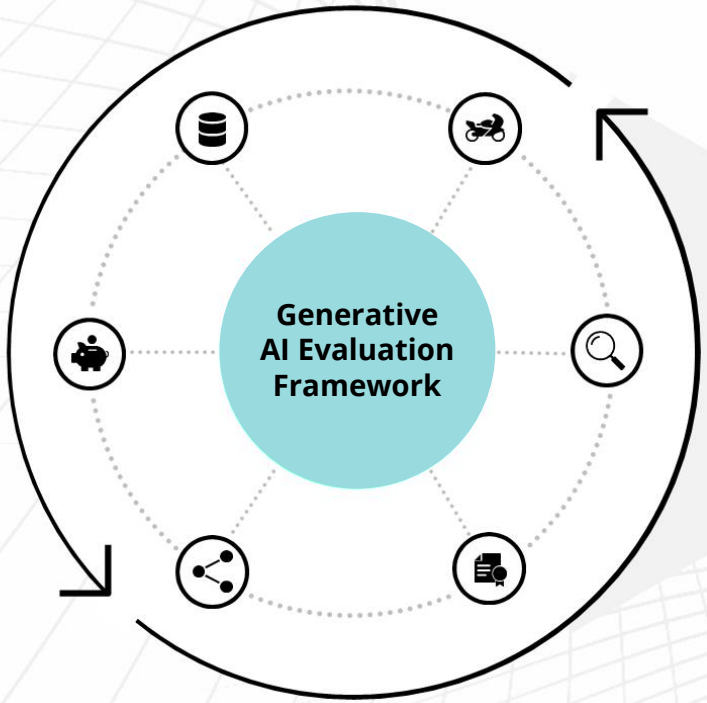


Data is only as good as our ability to find, interpret, and utilize it.

Thank You!

Better Health, Brighter Future

Introducing the Feasibility and Risk Framework



Dimension	Evaluation Factor	Considerations
ABILITY TO EXECUTE	**Data Availability & Quality**	✓ Are large volumes of clean data available that can be utilized as samples for GenAI training? ✓ Is a high diversity of data available to mitigate bias potential? ✓ How difficult is it to obtain and access data?
	Process Standardization & Governance	✓ Are the target processes well documented? ✓ Do the target processes contain known "accurate" and "inaccurate" outcomes that can be used to evaluate the GenAI model's performance?
	Nature of Input Prompts & Expected Outputs	✓ How frequent and complex are the outputs of the GenAI model? (e.g., 20-page documents vs. bullet points) ✓ Will system integrations be required to facilitate data inputs or outputs interpretations?
	Change Management	✓ Is the usability of GenAI embedded in the e2e process- and application landscaope providing a seamless user experience? ✓ Is the impact of workload and –content to the employees and the organization known and well managed to avoid lack of adoption?
DEGREE OF RISK	**Bias**	✓ Is my data over/under representative of a population cohort, region, gender, demographic group? ✓ Can steps be taken to mitigate bias during training? Are there any metrics that will be used to track bias? ✓ What level of impact criticality a biased output would have on the end user?
	Ethical Use	✓ Is an appropriate process in place ensuring that the model does not tread across lines of plagiarism and copyright violations? ✓ Will the solution be subject to independent oversight and review ensuring responsibility?
	Hallucination	✓ Is there a possibility to assess and validate attributions to the source information? ✓ Is an appropriate governance model in place to ensure the "human-in the loop"? (e.g., workforce upskilling, structured oversight, ubiquitous documentation)
	Cybersecurity	✓ Have the risks for data exfiltration, Data/Model poisoning, model stealing and adversial attacks being addressed? ✓ Is there a security architecture in place that addresses the key areas of security control Infrastructure and Network, Access Management, Monitoring and Data Protection?
	IP Protection	✓ Will information be shared with third parties through prompt engineering resulting to potential data leakage?
	Patient Health and Safety	✓ Is the model capable to process and provide medical information in prescience manner to avoid mistakes which can lead to adverse consequences to human health? ✓ Can the model consider appropriate emotional tone in the conversation to account for individual health status and ability to understand information?

What action will you and your organisation take?

Thank you!

https://mkto.deloitte.com/Intelligent-Health-booth.html