Generative AI oder doch lieber selber denken” - what do you think?

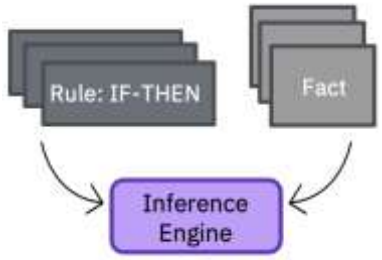
Thomas Jirku (IBM)
Technical Sales
thomas.jirku@at.ibm.com

prompt: an ibm machine that generates ideas in style of GREGORY CREWDSON

A little history on AI

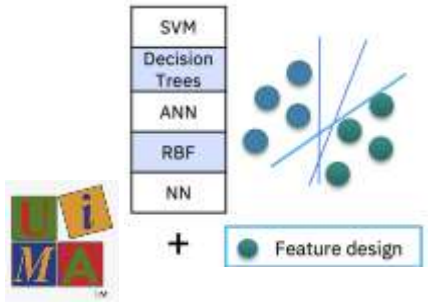
1980s

Big data
+
Small compute



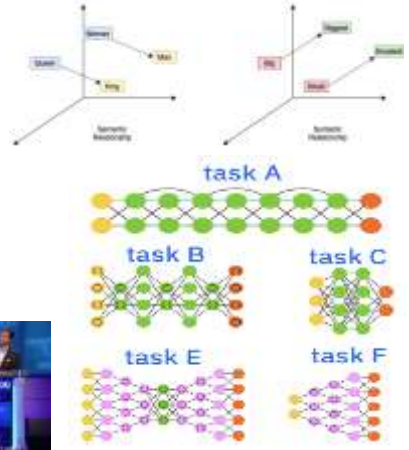
1980s to ~2010

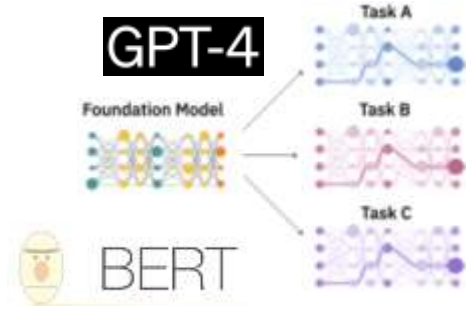
Massive labeled data
+
Compute



2017+

Self-supervision at scale
+
Massive **un**labeled data
+
Compute





Expert Systems

Hand-crafted symbolic representations

Machine Learning

Task-specific hand-crafted feature representations

Deep Learning

Task-specific learnt feature representations

Foundation Models

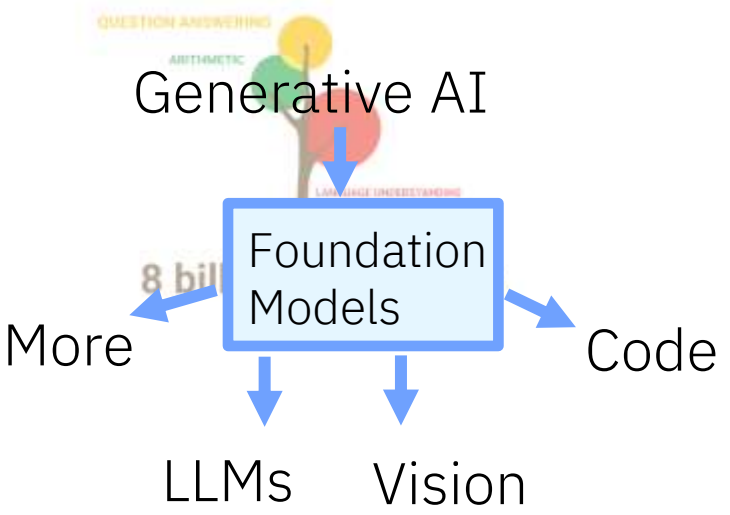
Generalizable & adaptable learnt representations

(often synonym to Large Language Models as most popular application is with language)

Foundation Models are…

- **Pre-trained** on unlabeled datasets of different modalities (e.g., language, time-series, tabular)
- Leverage **self-supervised learning**
- Learn **generalizable & adaptable data representations** which can be effectively used in **multiple downstream tasks**
  (e.g., text generation, machine translation, classification for languages)

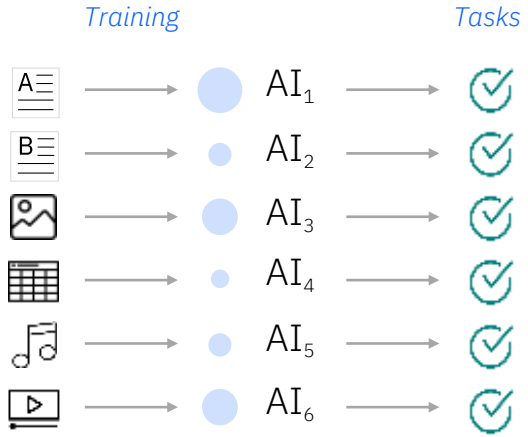
Note: while transformer architecture is most prevalent in foundation models, definition not restricted by model architecture



Inspired from Kate Soul's YouTube VIDEO

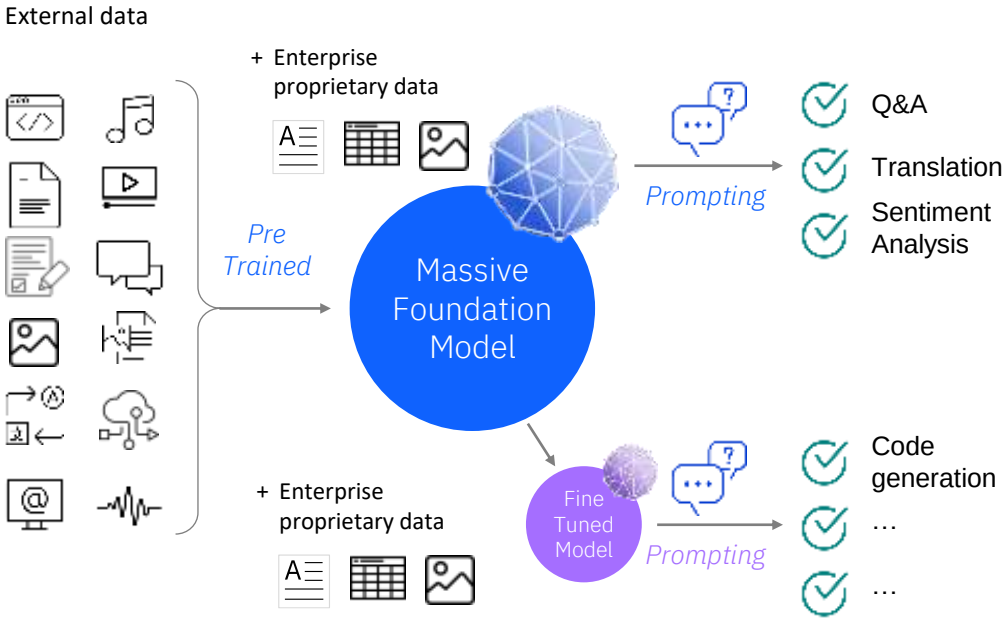
Foundation models establish a new paradigm for AI capabilities

Traditional AI models



- Individual siloed models
- Require task specific training
- Lots of human supervised training

Foundation Models



- Massive multi-tasking model
- Adaptable with minimized training
- Pre-trained unsupervised learning

Enhanced capabilities

- Summarization
- Conversational Knowledge
- Content Creation
- Code Co-Creation

Key advantages

- Lower upfront costs through less labeling
- Faster deployment through fine tuning and inferencing
- Equal or better accuracy for multiple use cases
- Incremental revenue. through better performance

up to 70% reduction
in certain NLP tasks

explainability

fairness

robustness

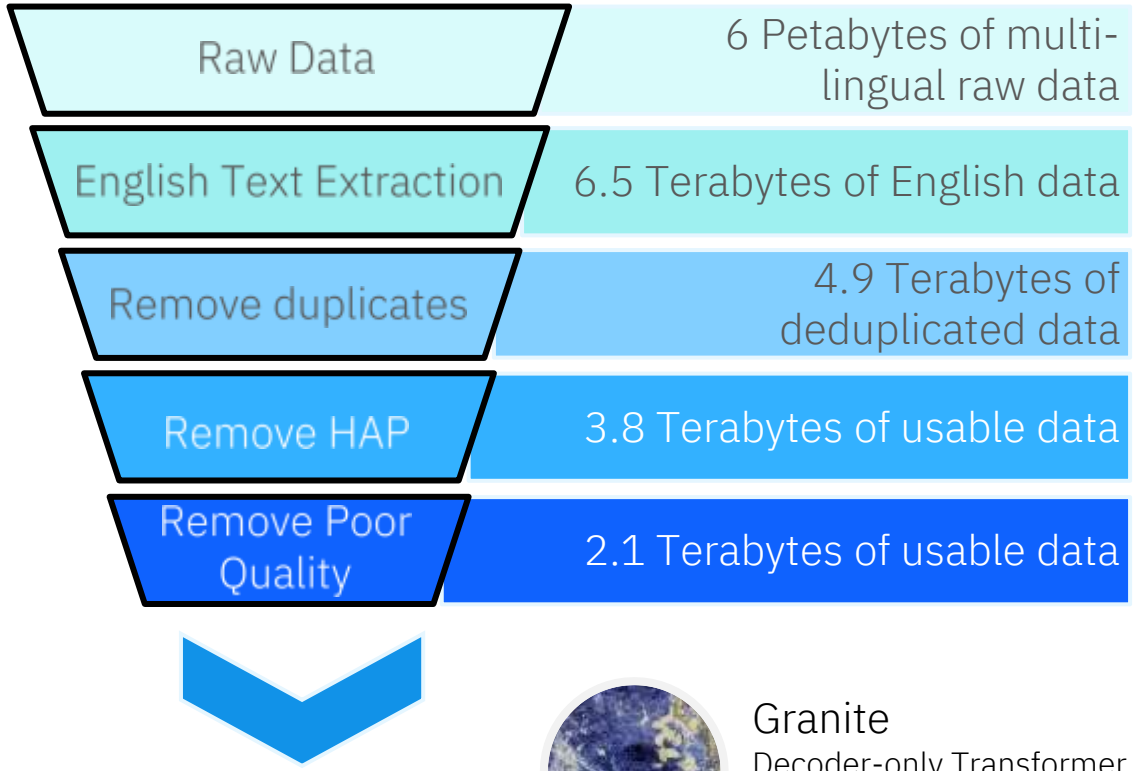
transparency

Granite LLM's on **watsonx.ai**

Trusted

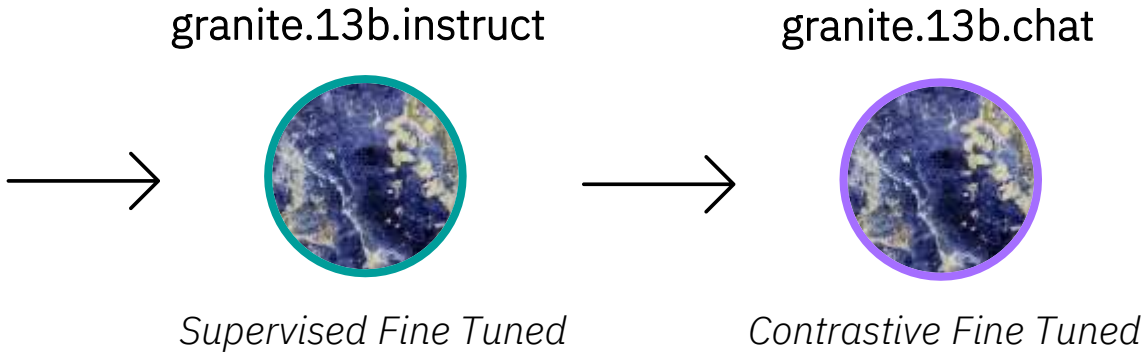
IBM's approach to AI model development is grounded in core principles of trust and transparency.

What were the datasets and sources used?

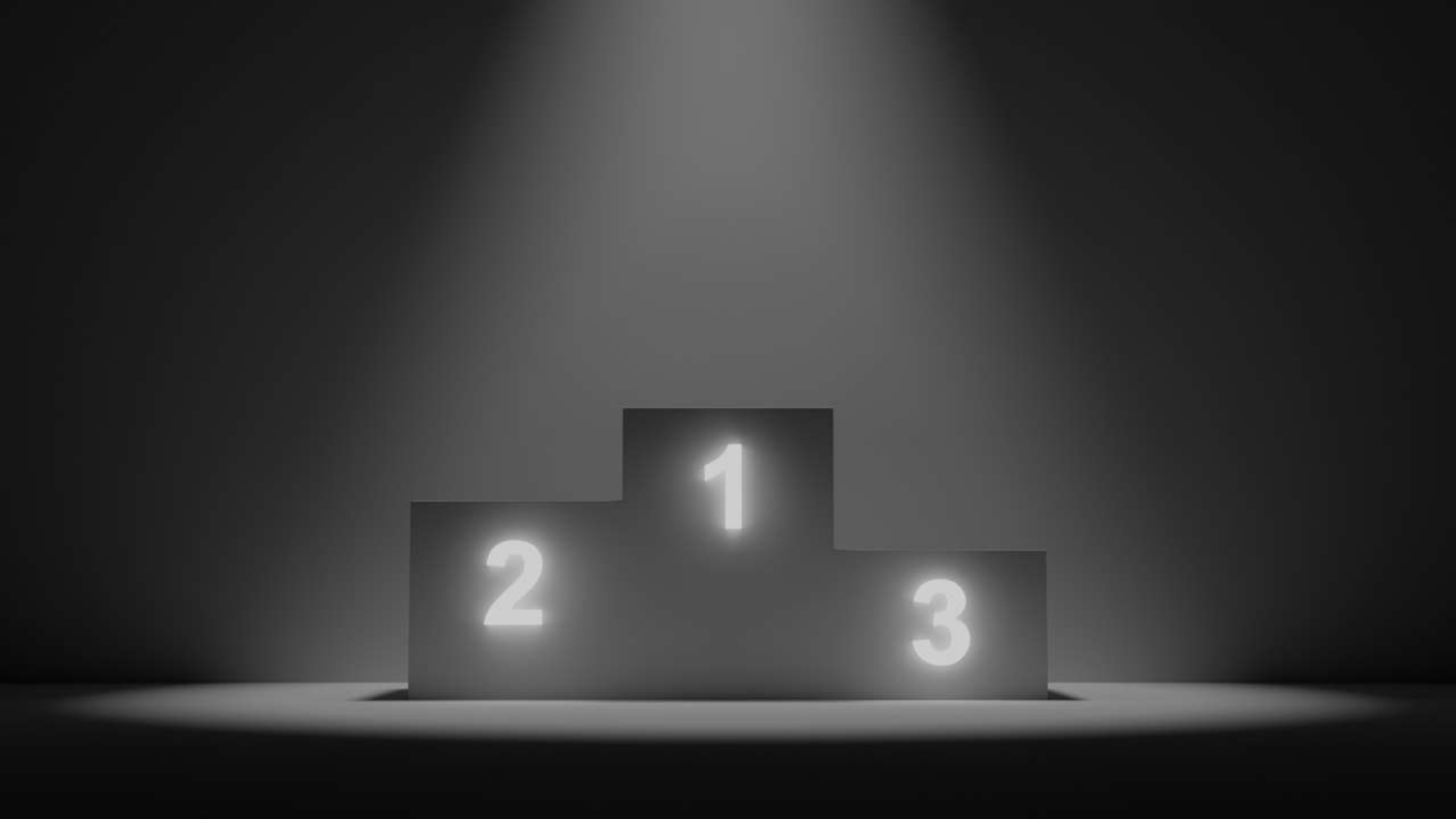


What makes IBM models safe for enterprise use?

- Models were reviewed against IBM's extensive data governance practices, corresponding to data clearance and acquisition; document quality checks; pre-processing data pipelines, including tokenization, data de-duplication, etc.
- Granite models were trained on data scrutinized by IBM's own HAP detector – to detect and root out objectionable content, benchmarked against internal and public models
- IBM deploys regular, ongoing data protection safeguards, including monitoring for websites known for piracy or other offensive materials, and avoid those websites



HAP – Hate Abuse and Profanity


2
1
3

EU AI ACT will highly regulate critical AI models

European Commission has outlined AI regulations that lay down

- harmonized rules for market placing, go-live and use of AI
- prohibitions for “unacceptable risk”
- requirements for “high-risk”
- harmonized transparency rules for “limited risk”
- rules on monitoring, market surveillance and governance
- measure in support of innovation

Regulation applies to:

- providers placing systems/services in EU regardless of location
- Users of AI systems in EU
- Providers and users of AI where output of the system is used in the EU


EUROPEAN COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

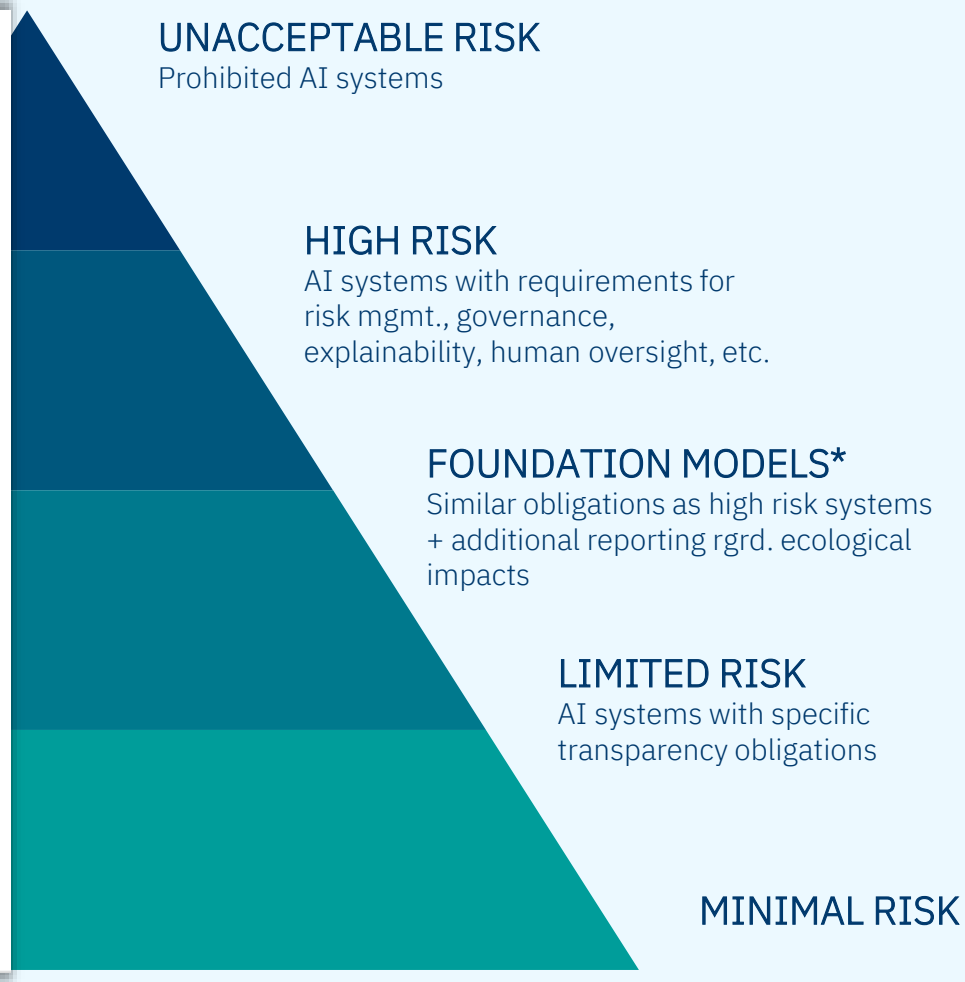
Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EN EN




MIND

Thomas Jirku, IBM

Thank you!

LinkedIn