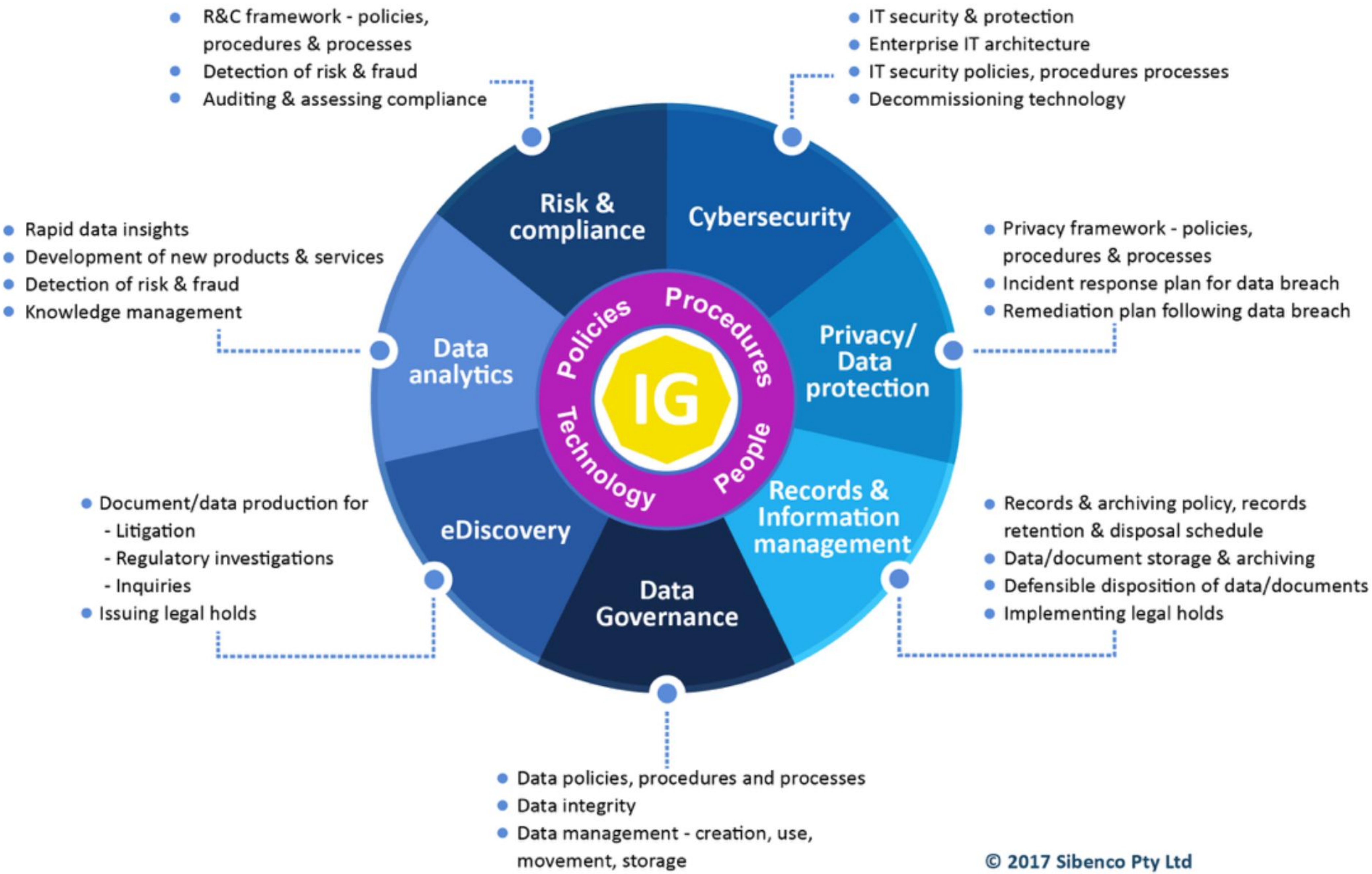
sampson.info/
2025-iolta-ai

Lee’s disclaimer

- The views, opinions, and information I share in this presentation are solely my own. They do not reflect the views, positions, or policies of my employer or any organization with which I am affiliated. Nothing presented should be taken as representing official statements on their behalf. Information about Maryland Judiciary projects is shared with permission.

AI Use Policies

Information Governance



IG

Policies

Procedures

People

Technology

Risk & compliance

- R&C framework - policies, procedures & processes
- Detection of risk & fraud
- Auditing & assessing compliance

Cybersecurity

- IT security & protection
- Enterprise IT architecture
- IT security policies, procedures processes
- Decommissioning technology

Privacy/ Data protection

- Privacy framework - policies, procedures & processes
- Incident response plan for data breach
- Remediation plan following data breach

Records & Information management

- Records & archiving policy, records retention & disposal schedule
- Data/document storage & archiving
- Defensible disposition of data/documents
- Implementing legal holds

Data Governance

- Data policies, procedures and processes
- Data integrity
- Data management - creation, use, movement, storage

eDiscovery

- Document/data production for
  - Litigation
  - Regulatory investigations
  - Inquiries
- Issuing legal holds

Data analytics

- Rapid data insights
- Development of new products & services
- Detection of risk & fraud
- Knowledge management

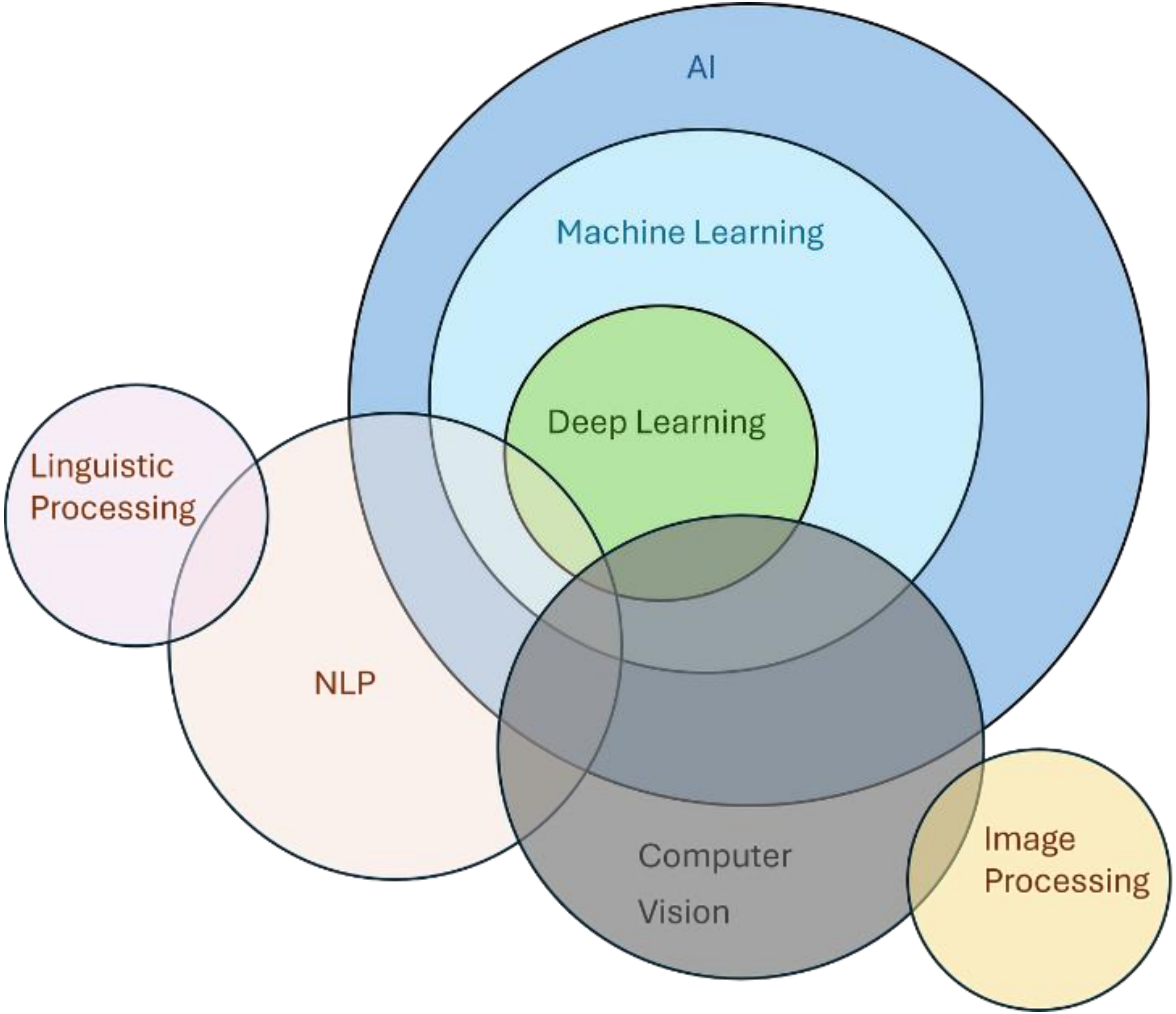
Elements of a GenAI Policy

1. **Purpose and scope**
2. **Governance and oversight**
3. **Data classification and handling**
4. Authorized GenAI tools
5. Authorized uses of GenAI tools
6. Prohibited uses of GenAI tools
7. **Training and competence**
8. **Security and confidentiality**
9. **Policy violations**
10. **Review and auditing**

Purpose and scope

- Mandatory section

- Defines the **organization's philosophy** and policy on use of GenAI.


AI
Machine Learning
Deep Learning
Linguistic Processing
NLP
Computer Vision
Image Processing

Governance and oversight

- Mandatory section

- Defines the **ultimate arbiter** of data classification and GenAI use.

Data classification and handling

- Mandatory section
- Establishes a **multi-tiered data classification** system with **escalating restrictions** on how each data type can be used with GenAI tools.

Data Classification	Definition	Acceptable AI Use
Public Data	Public Data includes any information that is publicly available, including information on the MLSC website. This includes information that grantees submit to MLSC with the understanding that it is public, including responses to reporting questions noted to be public.	Public Data may be uploaded to or used as input for any tool.
Internal Data	Internal Data is non-public information that MLSC receives or holds during its operations, but that does not meet the definition of Sensitive or Restricted Data. This generally includes grantee submissions, reports, audits, etc.	Internal Data may be ONLY uploaded to or used as input for MLSC Approved AI Tools.
Sensitive Data	Sensitive Data includes financial account information connected with any individual, organization, or business; human resources related data; and notes or recordings, if expressly stated to be confidential, of internal meetings or grantee communications.	Sensitive Data may be ONLY uploaded to or used as input for MLSC Approved AI Tools, and only with written approval from a member of the Executive Team.
Restricted Data	Internal MLSC records that include staff's date of birth, social security numbers, health related information, performance reviews or disciplinary actions.	This data may NOT be uploaded to or used as input for any AI tool.

Authorized GenAI tools

- Optional section

- Provides list of **GenAI tools** that are **authorized for use** by staff.
- Alternatives
  - **Allow list** where only these tools may be used
  - **Block list** where these tools may not be used

Authorized uses of GenAI tools

- Optional section

- Designates specific applications or workflows where **GenAI use is allowed**.

- Options include legal research, document drafting, administrative tasks, etc.

Prohibited uses of GenAI tools

- Optional section

- Designates specific applications or workflows where **GenAI use is not allowed**.

Training and competence

- Mandatory section

- Establishes that GenAI tools may only be used by staff who have who have **sufficient competency** to use GenAI tools in compliance with this policy.

Security and confidentiality

- Mandatory section

- Reminder of ongoing ethical and confidentiality concerns, stressing need to always be mindful of data classifications and authorized and prohibited uses.

Policy violations

- Mandatory section
- Establishes consequences for policy violations.

Review and auditing

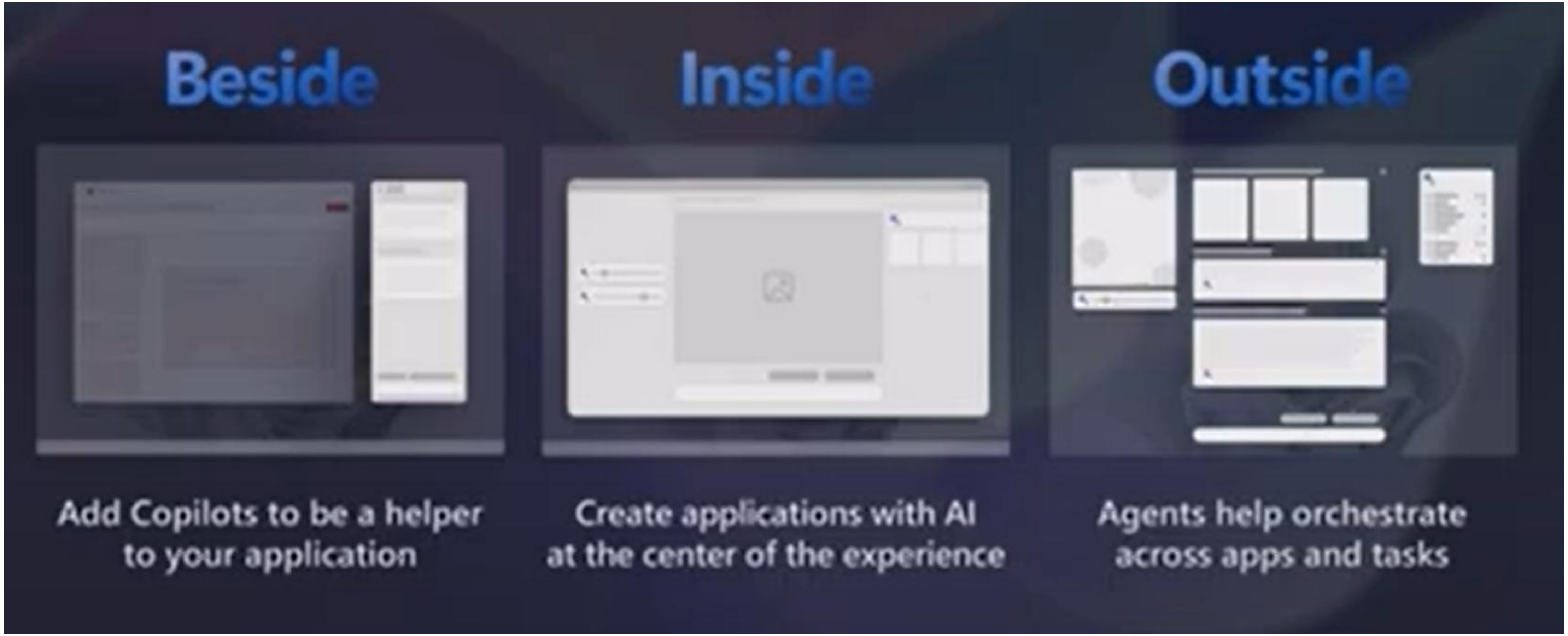
- Mandatory section

- Defines how the GenAI Governance Officer will **monitor use** of GenAI tools by staff and **build checks into workflows** to catch any errors that may be produced by GenAI tools.

Template available on website

Looking ahead

Beside, Inside, Outside



Beside

Add Copilots to be a helper to your application

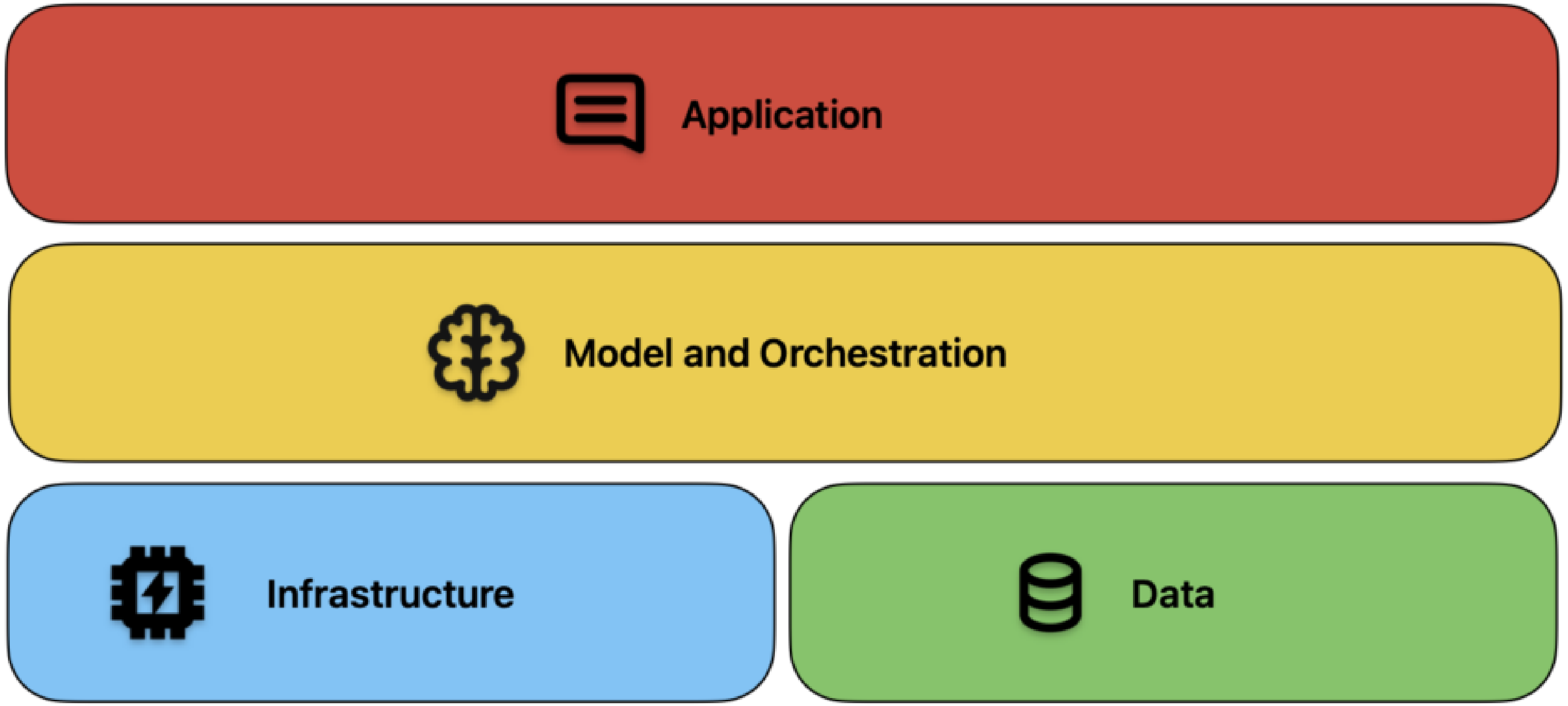
Inside

Create applications with AI at the center of the experience

Outside

Agents help orchestrate across apps and tasks

The AI Stack

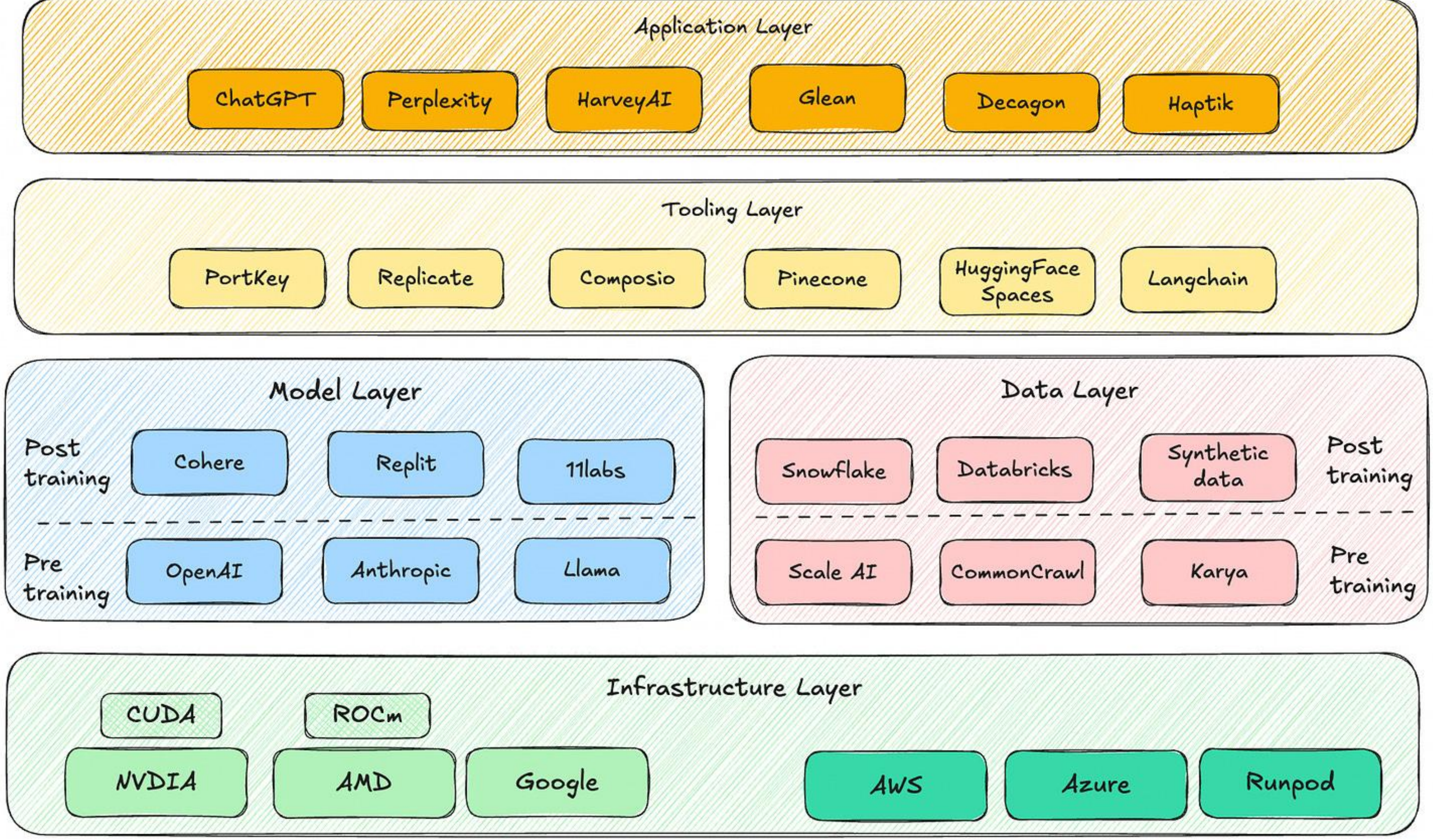


Application

Model and Orchestration

Infrastructure

Data


Application Layer
ChatGPT
Perplexity
HarveyAI
Glean
Decagon
Haptik
Tooling Layer
PortKey
Replicate
Composio
Pinecone
HuggingFace Spaces
Langchain
Model Layer
Post training
Cohere
Replit
11labs
Pre training
OpenAI
Anthropic
Llama
Data Layer
Snowflake
Databricks
Synthetic data
Post training
Scale AI
CommonCrawl
Karya
Pre training
Infrastructure Layer
CUDA
ROCm
NVDIA
AMD
Google
AWS
Azure
Runpod

First, do no harm (*Ferris v. Amazon*)

- Courts exist to decide controversies fairly, in accordance with the law. This function is undermined when litigants using AI persistently misrepresent the law to the courts. AI is a powerful tool, that when used prudently, provides immense benefits. When used carelessly, it produces frustratingly realistic legal fiction that takes inordinately longer to respond to than to create. **While one party can create a fake legal brief at the click of a button, the opposing party and court must parse through the case names, citations, and points of law to determine which parts, if any, are true**. As AI continues to proliferate, this creation-response imbalance places significant strain on the judicial system.

Hallucination tracker

- https://www.damiencharlotin.com/hallucinations/
- ChatGPT
- Gemini
- Copilot
- Claude
- Ghostwriter Legal
- **CoCounsel**
- **Lexis+AI**

Are hallucinations insurmountable?

- Why Large Language Models Hallucinate
- large language models sometimes guess when uncertain, producing plausible yet incorrect statements instead of admitting uncertainty.
- language models are optimized to be good test-takers, and guessing when uncertain improves test performance.

Trouble now and trouble later?

- Your grantee’s clients are using GenAI – what do we do?
- Educate about limits of ChatGPT?
- Ask OpenAI not to answer legal questions?
- Build a competitor?
- **What level of inaccuracy is acceptable?**