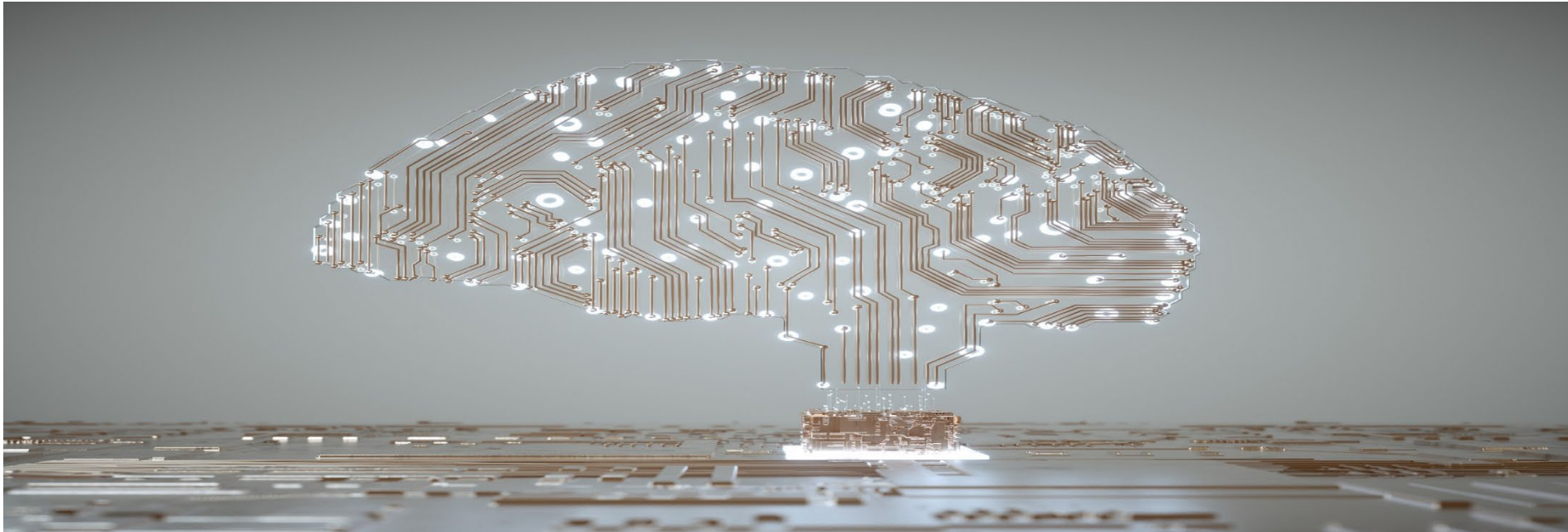
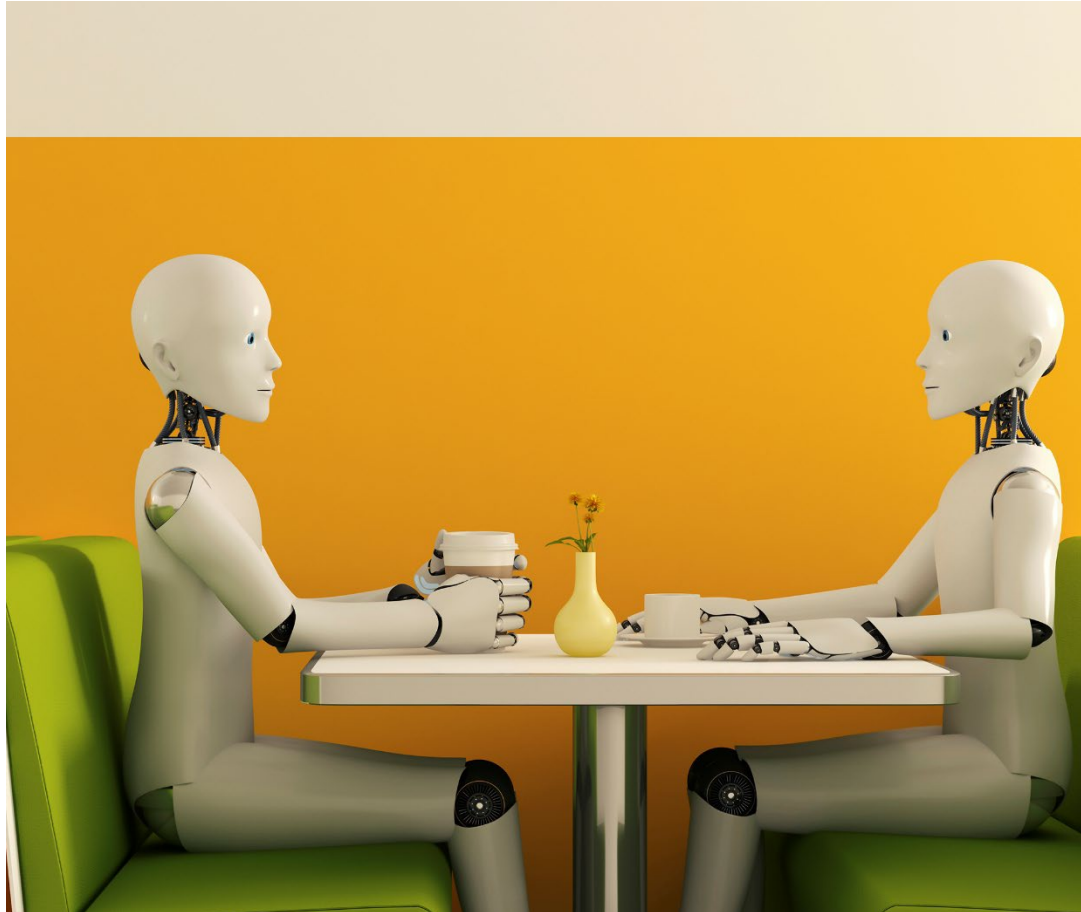


Artificial Intelligence (AI) in the Workplace: Managing Risks Through Effective Policy Design

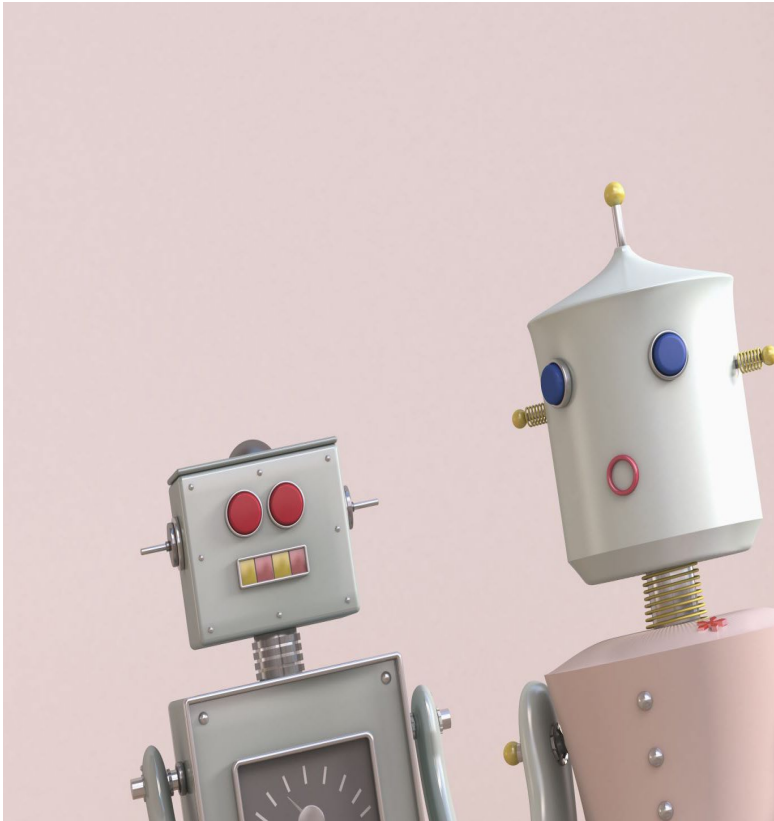


Agenda



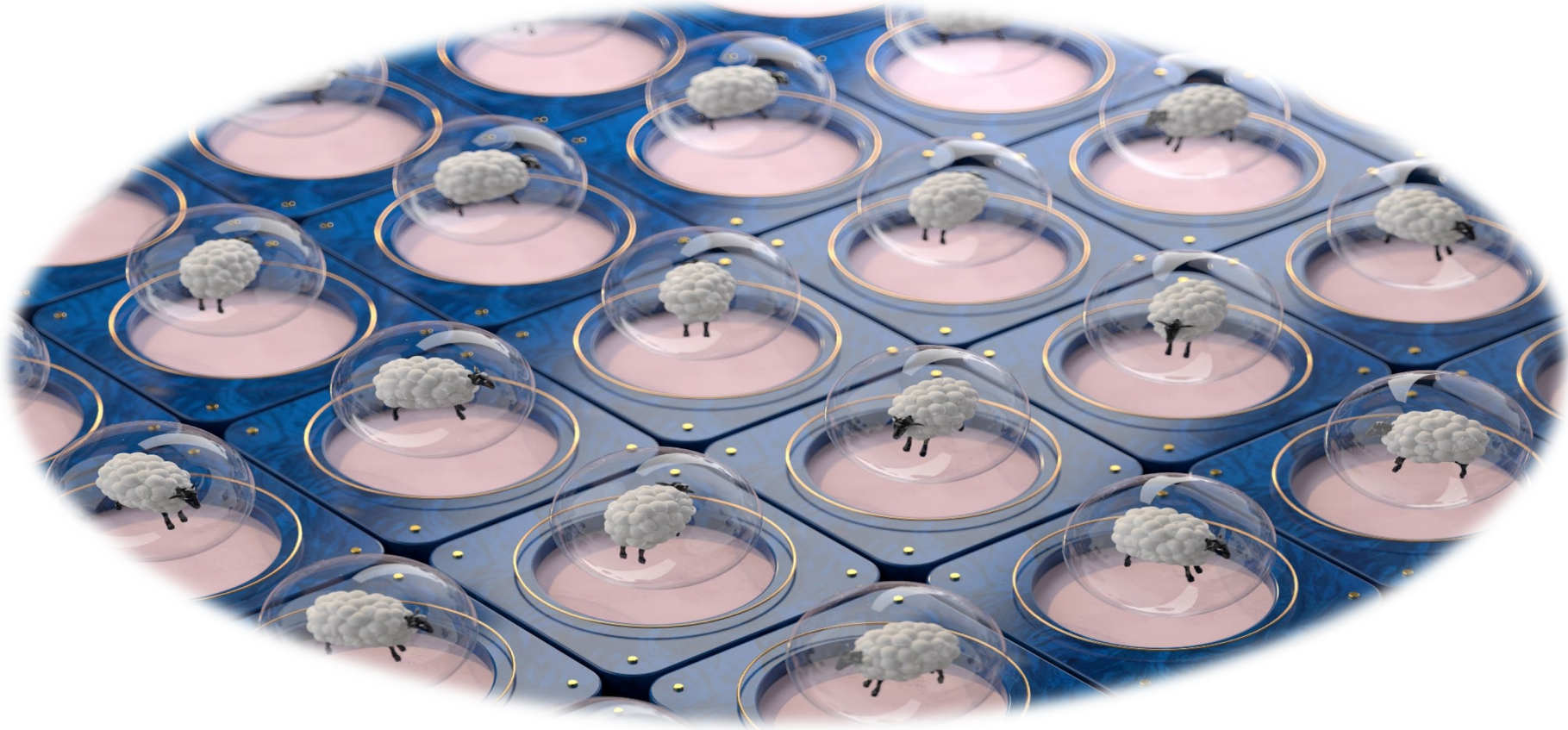
- What is Artificial Intelligence
- AI Risks and Liabilities
- AI Governance
- Anatomy of an AI Policy
- Q&A

Disclaimer

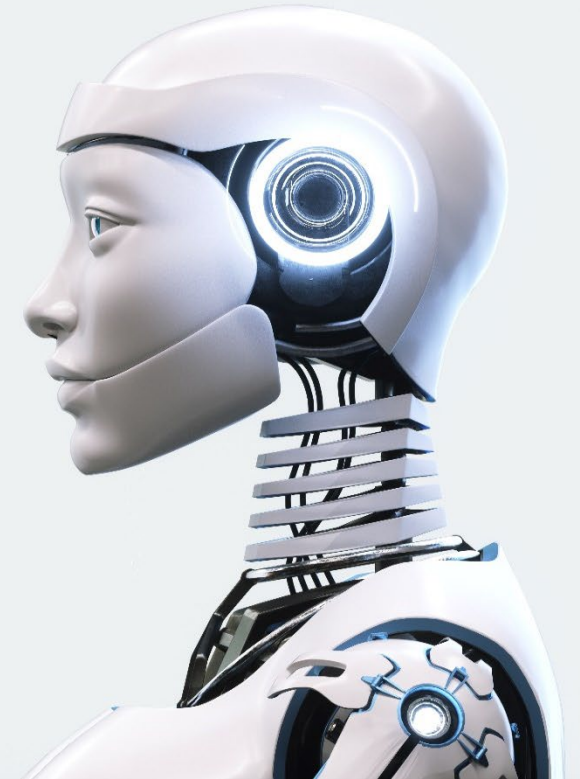
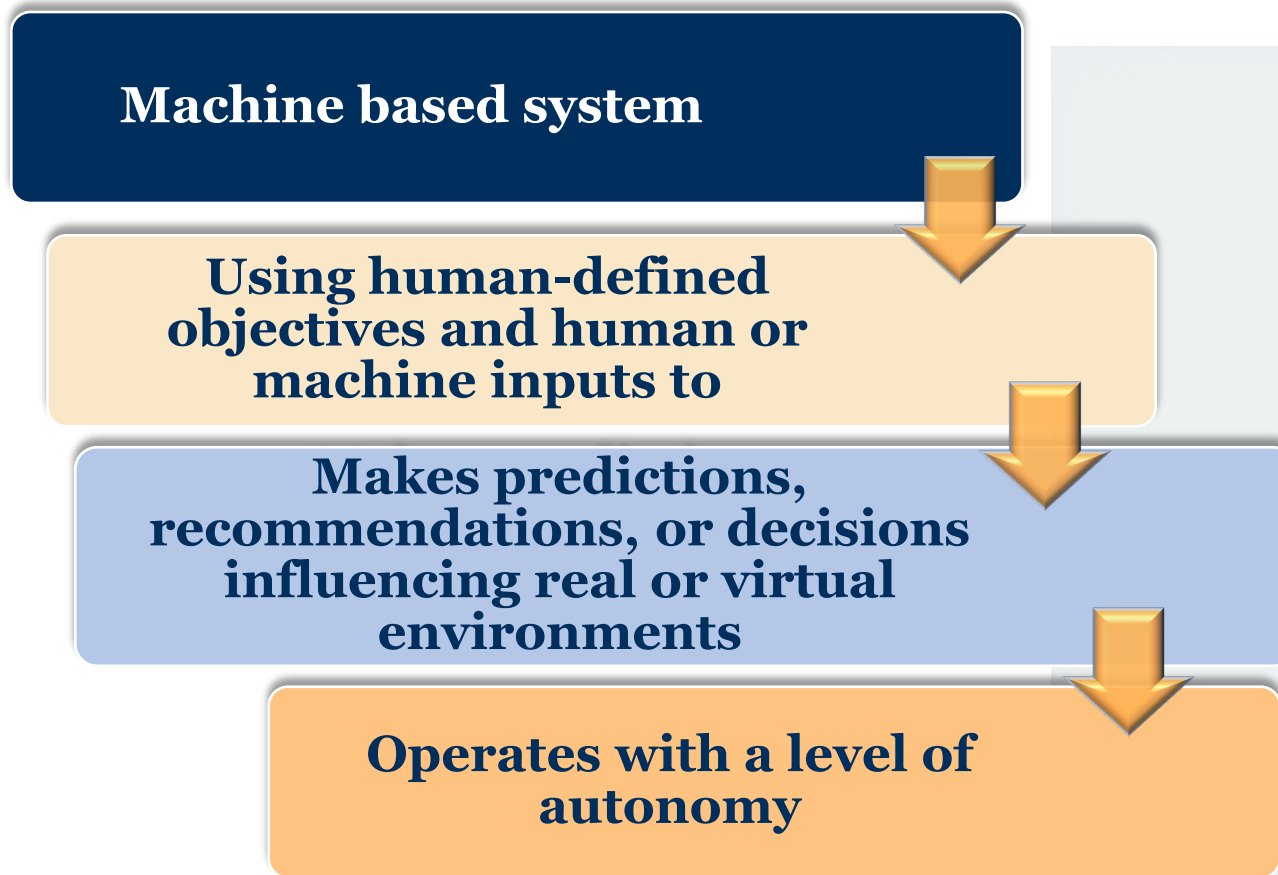


- This presentation is not intended to provide legal advice or to create an attorney-client relationship.
- All opinions expressed throughout this presentation are the presenter's personal views and do not necessarily reflect the opinion of Eckert Seamans.

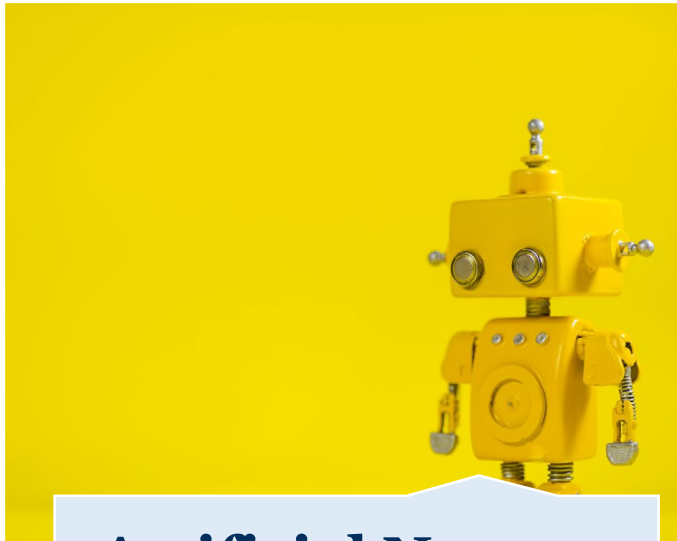
What Is Artificial Intelligence



Definition of AI



AI Classifications



**Artificial Narrow
Intelligence (ANI)**



**Artificial General
Intelligence (AGI)**



**Artificial Super
Intelligence (ASI)**

Common AI Systems

Generative AI (Gen AI) / LLMs

(Search Engines / Content Creation / AI Assistants / Companion AI)

Predictive Algorithmic Models

(Financial forecasting / insurance underwriting / fraud detection)

Robotic Processing Automation (PRA)

(manufacturing / call center operations / claims administration)

Expert Systems

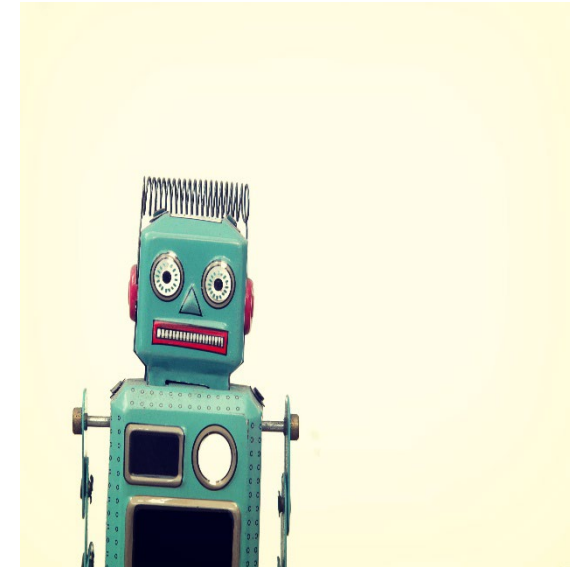
(Scientific research & medical diagnosis / Customer support)

Recommendation Engines

(Shopping / Product preferences / Advertising)

Autonomous or Agentic AI Systems

(Workflow automation / Risk assessment / Underwriting / Fraud detection / Dynamic pricing)



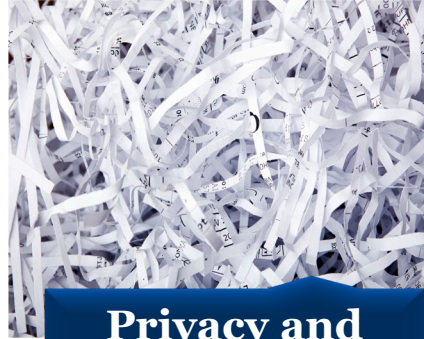
AI Risks



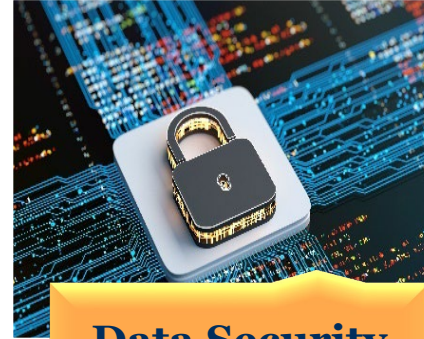
Potential Types of Harm



**IP / Data
Ownership**



**Privacy and
Confidentiality**



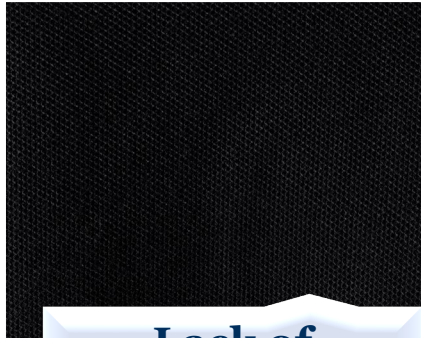
Data Security



**Discrimination
/ Bias**



**Inaccuracies /
Misinformation**



**Lack of
Transparency**

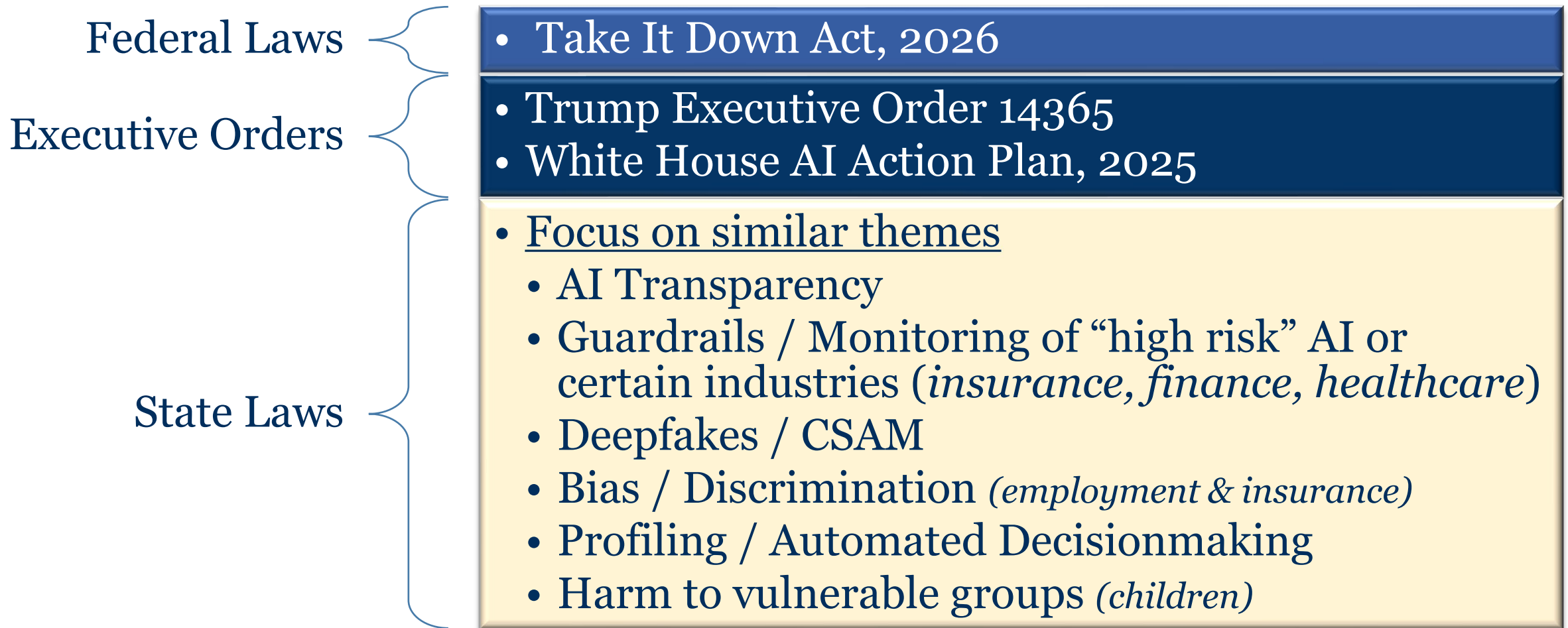


**Human Rights /
Ethics**

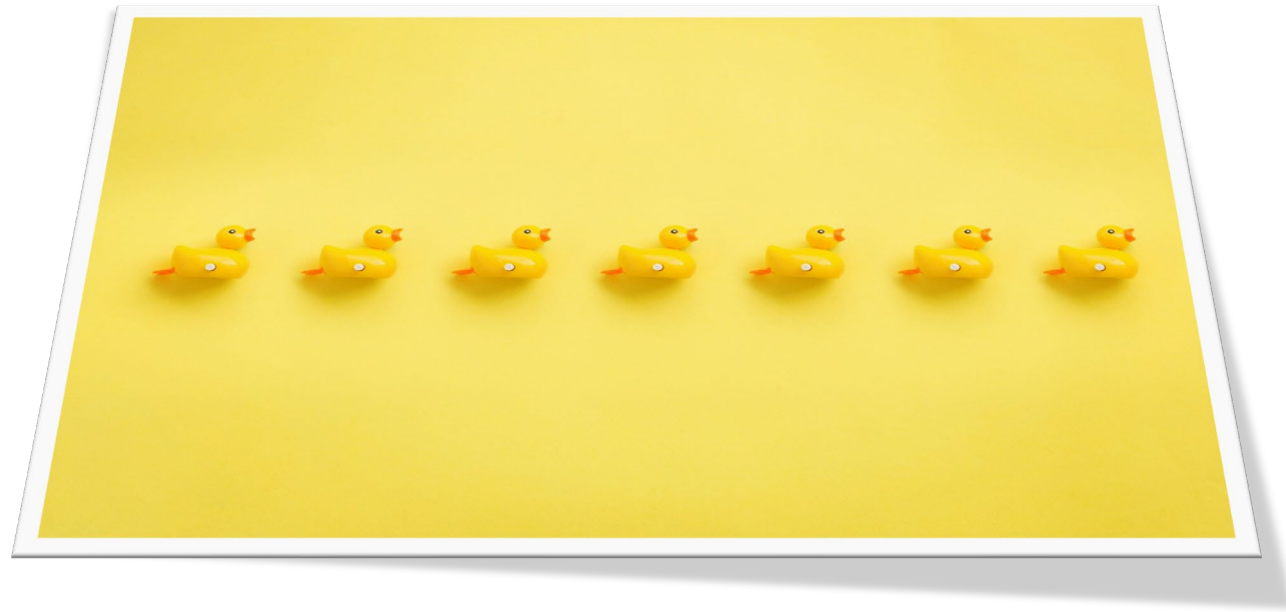


**Human Safety /
Harm**

AI Laws – Current US Landscape



AI Governance



AI Frameworks

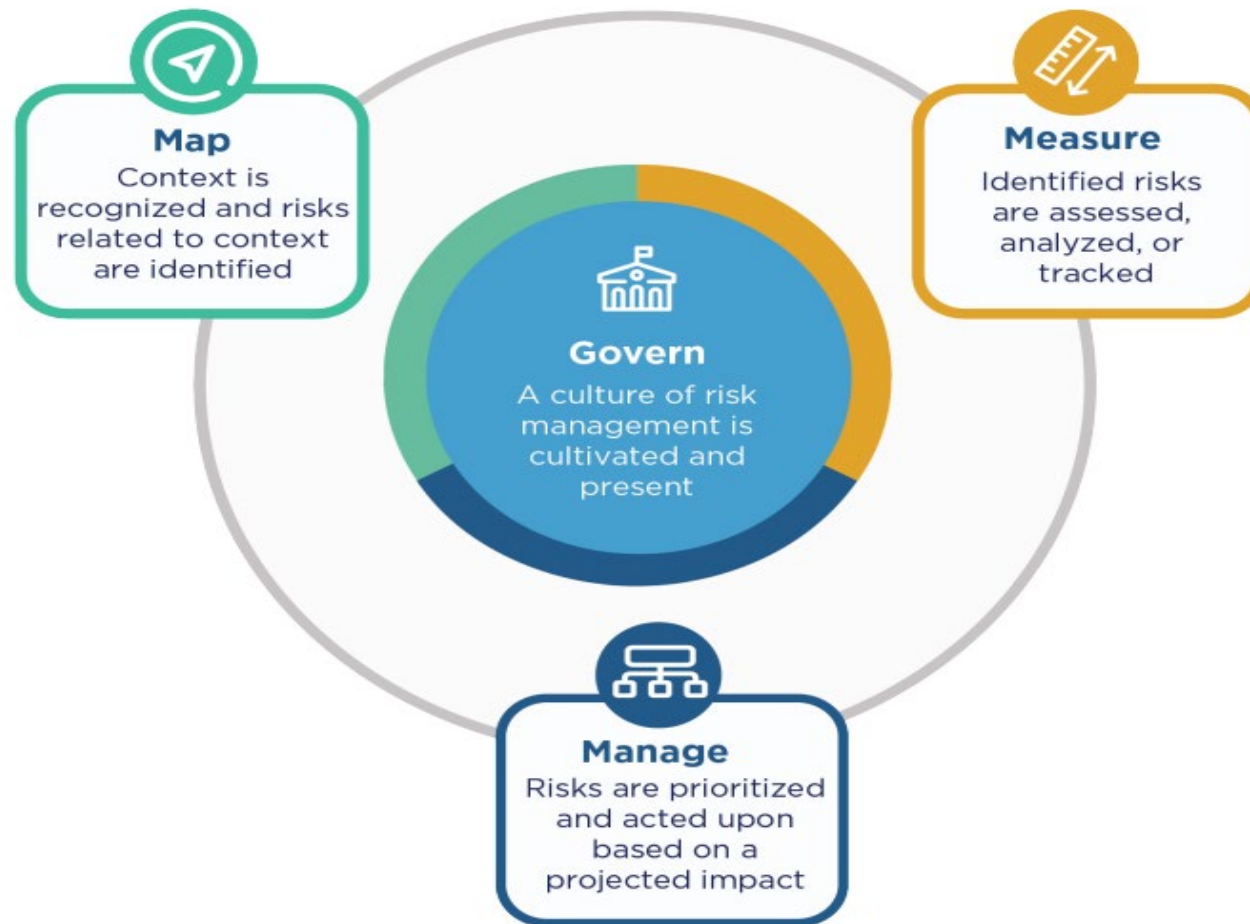
NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)



Fig. 4. Characteristics of trustworthy AI systems. Valid & Reliable is a necessary condition of trustworthiness and is shown as the base for other trustworthiness characteristics. Accountable & Transparent is shown as a vertical box because it relates to all other characteristics.

**Fig. 4 (p. 12) of the NIST AI RMF 1.0 available at:
<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>*

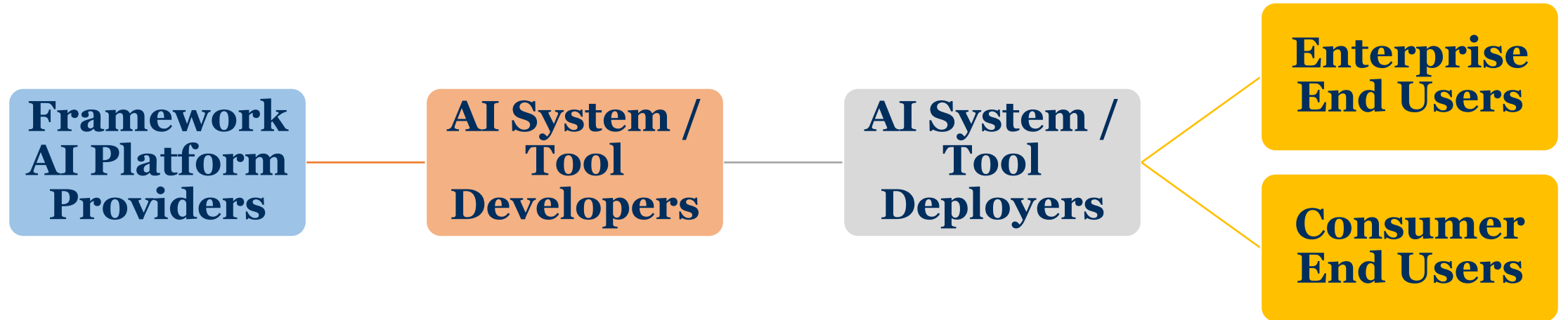
AI Frameworks



NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)

**Fig. 5 (p. 20) of the NIST AI RMF 1.0*

AI Product Lifecycle



Public vs. Enterprise AI

Public AI

- **Benefits:** Low cost, time, and resources to adopt
- **Risks:**
 - Privacy / Confidentiality / Cybersecurity risks
 - Subject to standard online terms
 - Less oversight and control

Enterprise AI

- **Benefits:**
 - Can negotiate more protective contract terms
 - More oversight & control (can perform due diligence)
 - Less cybersecurity and privacy / confidentiality risks
- **Risks:** Costly & Time / Resource intensive to implement

Organization Wide AI Governance Program



Establish AI Governance Leadership / Interdisciplinary team



Create an AI Risk Management Framework for the Adoption & Use of AI Tools



Adopt AI Policies for Staff



Analyze / Adopt Security Measures to Address AI Security Risks



Conduct Risk Management Assessments for New AI Tools



Maintain an Inventory of AI Tools



Adopt AI Specific Contractual Provisions in Third Party Contracts



Train Staff on the Ethical Use of AI

Anatomy Of An AI Policy

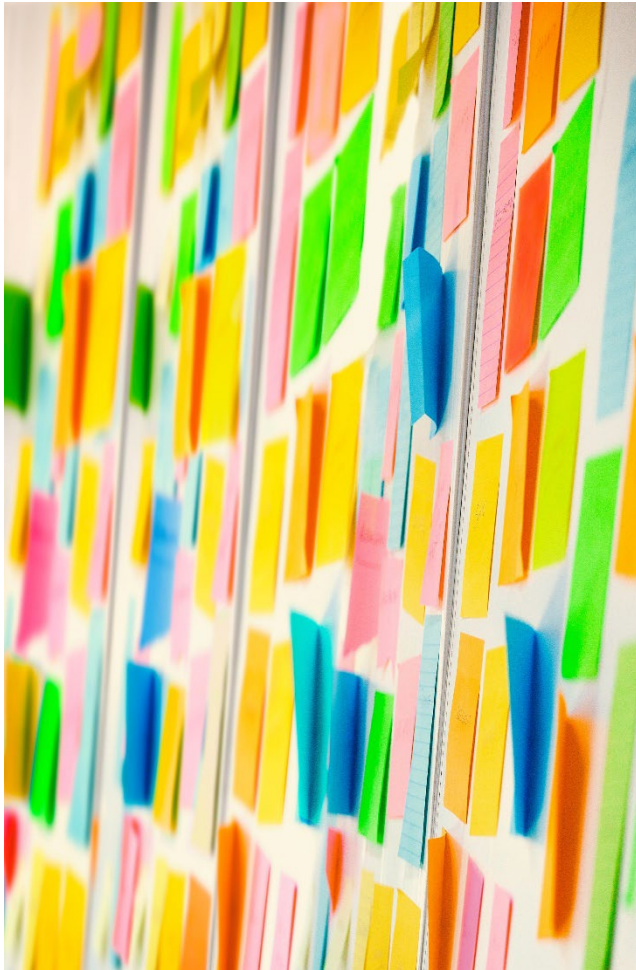


AI Policy Questions

- **What Laws / Rules Apply?**
- **What Tools are Permissible / Prohibited?**
- **What are the Permitted / Prohibited Use Cases?**
- **What Data Inputs is Permitted / Prohibited?**
- **What Procedures Must Users Follow to Ensure Ethical/Legal AI Use?**
- **What Procedures Should the Organization Employ to Ensure Compliance with the AI Policy?**
- **What Specific Use Cases Should Be Addressed?**



AI Policy – General Framework



- Defined Terms
- Policy Owner / Responsibility
- Policy Scope
- ***General Rules on using AI at Work***
- Employee Training
- Reporting Obligations / Consequences for Violating the Policy
- Policy Acknowledgement & Consent
- *Exhibits*
 - List of Approved AI / Permitted Purposes
 - List of Approved / Restricted Data Inputs
 - ***General AI Prohibited Purposes***
 - ***AI Use Procedures***
 - ***Rules for Specific Use Cases***

AI Policy – General AI Use Rules

- Only use approved AI tools on approved devices.
- Never input “*prohibited data*” & only use the minimum needed data.
- Never use any AI Tool for a “*prohibited purpose*”.
- Always follow the AI use procedures and specific use case rules.



AI Policy – Prohibited Purposes



What is prohibited may depend on the:

- Applicable law;
- Intended purpose; &
- Organization's risk tolerance.

AI Policy – Prohibited Purposes

Human

- Deceive or spread misinformation
- Harass or discriminate
- Impersonate another person
- Real time surveillance

Security

- Spam or create malicious code
- Infiltrate / compromise / circumvent computer systems or security features

Laws

- Terrorism / weapons
- Election integrity
- Deepfakes / CSAM

Liability

- IP infringement / web scraping
- Legal, financial, health, medical, tax advice

AI Policy – AI Use Procedures

- Confirm adherence to the “General AI Rules” when using AI.
- Review AI output for accuracy & confirm facts and sources cited in output.
- Review AI Output for prohibited content (e.g., IP infringing materials, offensive/discriminatory output, and biased conclusions).
- Document / save all prompts, inquiries, and documents imputed into the AI tool.
- Label AI output (e.g., AI name & version, reviewer name & review date, and any output modifications).
- Document decisions made (in whole or part) by AI and reviewed / confirmed decisions by a human.
- Disclose if communications were created using AI.

AI Policy – Specific AI Issues

AI Recordings



- Wiretap Laws

- Always obtain express consent of ALL parties to a meeting if using AI recording tools
(e.g., AI meeting note takers & wearables)

- Confidential / Privileged Discussions

- If the meeting may discuss privileged or potential confidential or sensitive personal information, ensure that AI recording tools are not active

AI Policy – Specific AI Issues

Open Records Laws

- May be subject to Open Records / AI Transparency Laws: AI inputs / prompts & outputs and AI meeting transcripts.
- Map applicable laws and address risk of confidential information becoming a public/agency record.
- Review / update document retention policies to ensure all AI materials and associated audit trail is retained / accessible.



Questions



ECKERT SEAMANS