iapp

AI Agents & Agentic AI - What Legal & Privacy Leaders Must Know Now

Thursday, July 10, 2025

8:00–9:00 PST

11:00-12:00 EST

17:00–18:00 CET

Welcome and Introduction

Panelist

Cassandra Maldini
AIGP, CIPP/US, CIPM, FIP
VP of AI Governance & Privacy
Securiti

Why Are We Here?

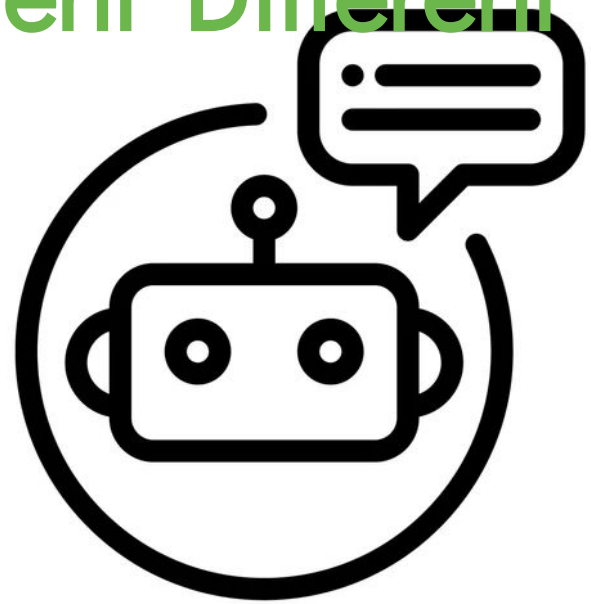
This **is not** an engineering lecture

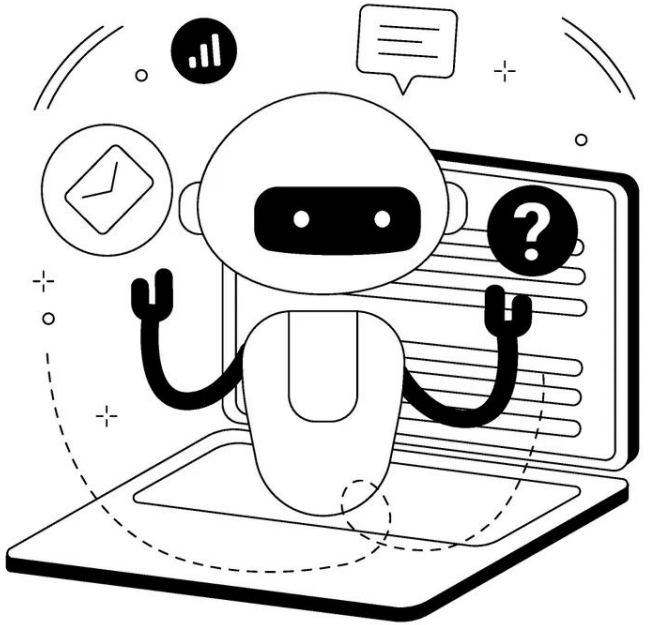
This **is not** a philosophical debate on AI hype v. AI doom

This IS a plainspoken guide for legal and privacy leaders to understand what is changing - and how to lead the build

OUR GOAL: To demystify AI agents and give you real tools and language to govern them, even if you're not vibe coding in your free time.

From Prompts to Plans - What Makes An AI Agent Different

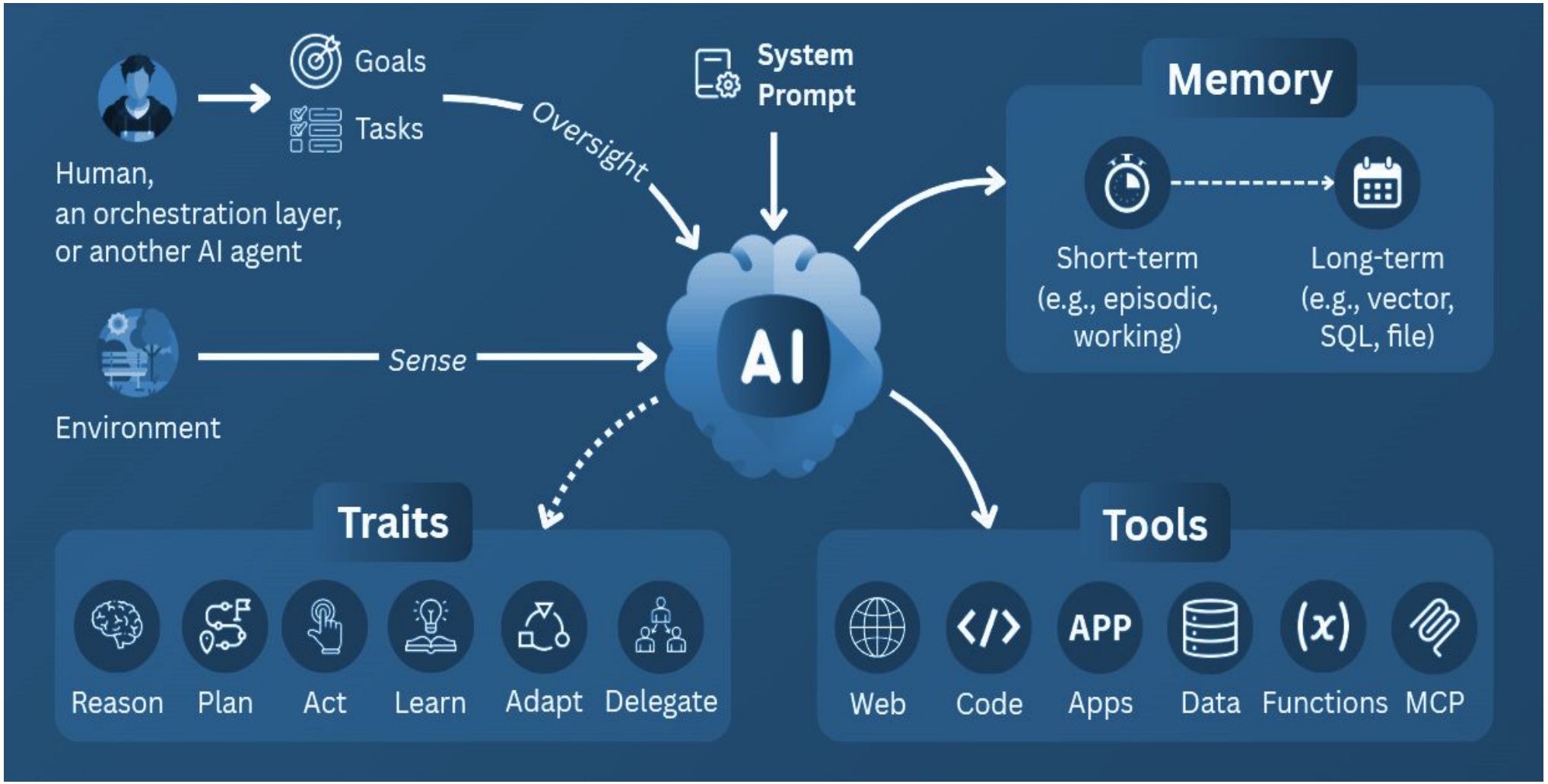




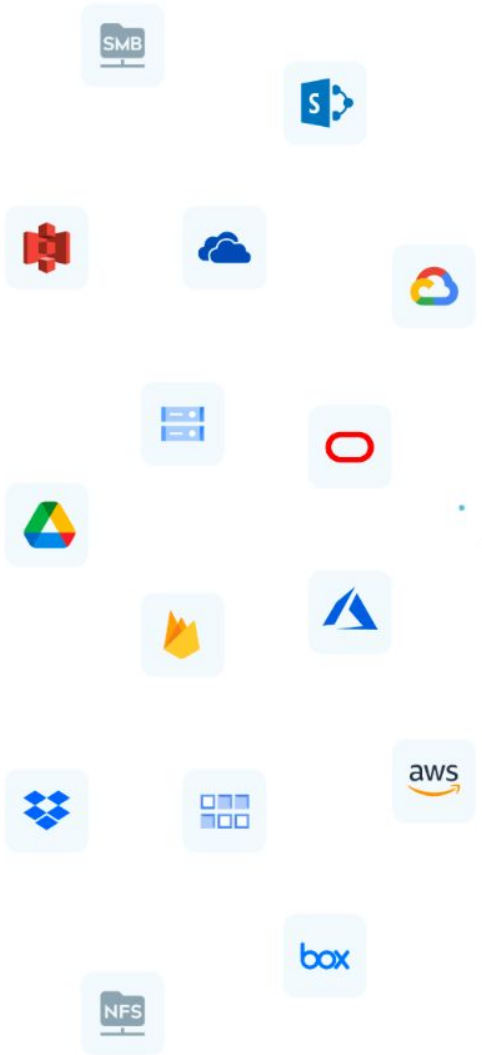
AUTOMATED
REACTIVE TO SINGLE PROMPT

AUTONOMOUS, GOAL-ORIENTED
TOOL USING, STATEFUL

Anatomy of an AI Agent



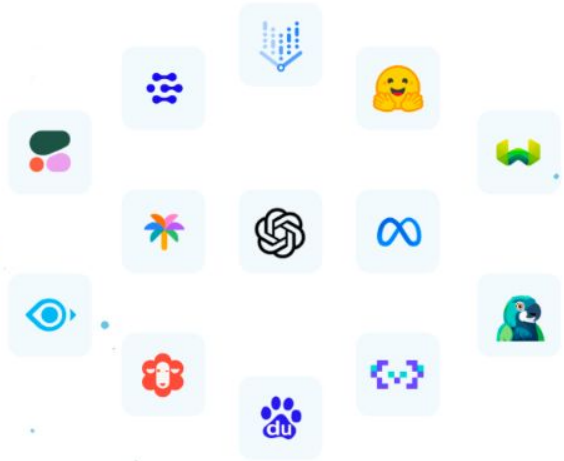
What data is being used in AI Models?



Are AI Systems Compliant with Global Regulations?

- EU AI Act
- CA AIDA
- US EO 14110
- US NY Law 144
- BR AI Law
- CN Interim Measures on Gen AI
- CN Algorithmic Recommendations Provisions
- SG Model AI Framework

Which AI Models, AI Agents & AI-X Exist in your Environment?



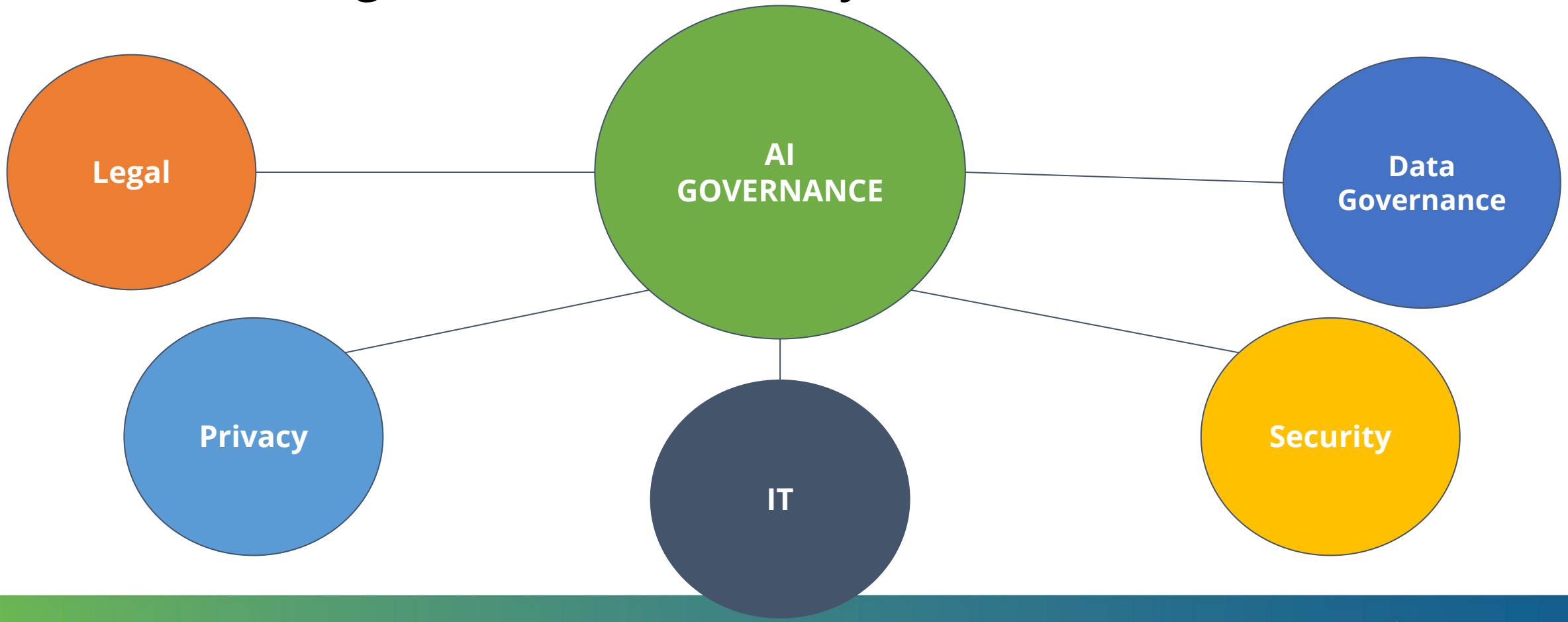
- Which security controls are enabled for AI Models & AI Agent?
- What is the Risk Rating of AI Models & AI Agents

What Controls are there on prompts, agents, assistants?

- AI Copilots & Assistants
- Business Process Automations
- Knowledge Creation
- Code

Let's Align on Terminology

Before we dive in, let's make sure we're on the same page.
What does AI governance mean to you?



Why The Freak Out Amongst Governance Pros

"[Agents] would need to be able to drive [processes] across our entire system with something that looks like root permission, accessing every single one of those databases — probably ***in the clear***, because there's ***no model to do that encrypted***,

And if we're talking about a sufficiently powerful … AI model that's powering that, there's no way that's happening on device," she continued. "That's almost certainly being sent to a cloud server where it's being processed and sent back. So there's a ***profound issue with security and privacy that is haunting this hype around agents, and that is ultimately threatening to break the blood-brain barrier between the application layer and the OS layer by conjoining all of these separate services [and] muddying their data***," (Meredith Whitaker, CEO, Signal, SXSW Austin March 2925

Where Things are Breaking Today

- Hallucinated Outputs
- AI Tool Misuse
- Privacy Violations
- Sensitive Data Exposure
- Sloppy Access Management (RBAC)
- Bias & Fairness Concerns
- Transparency Concerns
- AI First = Ask Forgiveness
- No human in the loop
- Lack of oversight or governance processes
- Data Quality - junk in/junk out
- Legal brought in late
- Legal = checkers Product/Enterprise = 3D Chess
- Velocity
- Relaxed REgulatory Environment

So what can we do about this mess? Key practical takeaways

From Fear to Control: 5-Step Approach to AI Security & Governance

STEP 1

Discover Shadow AI (X)

Discover and catalog sanctioned and unsanctioned AI models, AI Agents, AI-X across public clouds, private environments, and SaaS applications.

STEP 2

Assess AI and AI Agent Risks

Evaluate risks related to data and AI models from IaaS and SaaS, and classify AI models & AI Agents as per global regulatory requirements.

STEP 3

Map Data+AI Flows

Connect models to data sources, processes, vendors, potential risks, and compliance obligations.

STEP 4

Implement Data+AI Controls

Establish data controls on model inputs and outputs, securing AI systems from unauthorized access or manipulation.

STEP 5

Comply with Confidence

Conduct assessments to comply with standards such as NIST AI RMF, the EU AI Act, and more.

Shadow AI /Un-Sanctioned & Sanctioned AI — **Sanctioned**

A Very Non-Exhaustive List of Questions to Ask About AI Agents

WHAT TOOLS CAN IT USE?

WHAT DATA CAN IT TOUCH?

WHO IS HANDLING ACCESS CONTROLS & ARE THEY AIRTIGHT?

WHAT IS THE INTENDED PURPOSE?

CAN THE AGENT HALLUCINATE ACTIONS, NOT JUST TEXT?

IS THERE A KILL SWITCH?

Web Conference
Participant Feedback Survey

Please take this quick 2-minute survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iapp.questionpro.com/t/ACtQeZ6VnT

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation please
contact:

livewebconteam@iapp.org