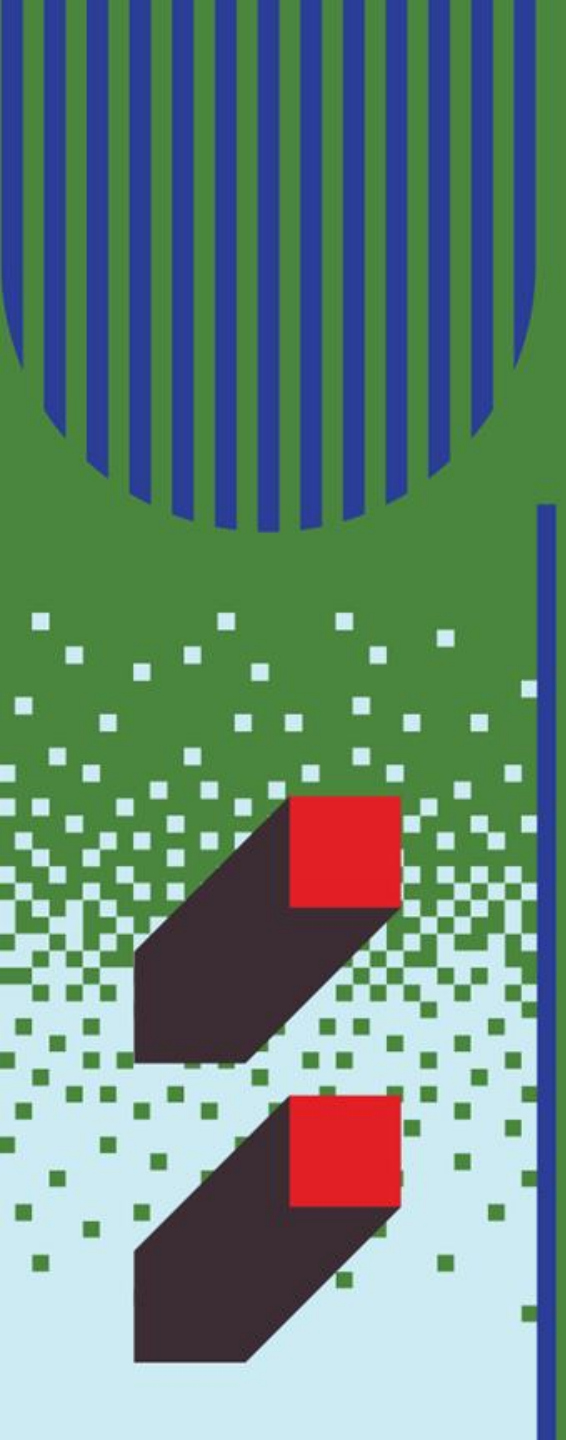

IAPP Global Summit 2026

Privacy | AI governance | Cybersecurity law

Conference 30-31 March

Workshops 1 April

Training 1-2 April

WASHINGTON, DC

#IAPPSummit26

Guidelines to Guardrails: Governing Agentic AI in Practice

AGENDA

- Introductions and Level-Setting
- Agentic AI Use Case
- Architecture and Data Flow
- Discussion
- Audience Questions

What is Agentic AI?

- Acts with autonomy
- Uses multi-step reasoning without constant human supervision
- Plans, adapts, and executes
- Tell me something vs DO something

Proof of Concept to Production

Use case: An AI engine monitoring ‘promises’ we make to our customers during contact center interactions and ensuring they are fulfilled

POC Stage

- Feasibility of accuracy
- Cost of a mistake
- Evaluate tool and data access
- Responsible AI triage

Development

- Integration with systems of action
- Human in the loop change management
- Agent implementation

Production

- Performance monitoring
- Model release management
- IT changement management

Proof of Concept to Production

Use case: An AI engine monitoring ‘promises’ we make to our customers during contact center interactions and ensuring they are fulfilled

Data

- Interaction transcript
- Service agreements
- Customer bill
- Ticketing systems

Action examples

- Detect call-back promise from agent, check for ticket creation, create ticket if required
- Check for activation fee waiver, confirm alignment with service agreement, alert back office agent if required

Key Considerations

- Consent capture to analyze call
- Human in the loop for high impact actions
- Ongoing monitoring for performance drift
- Traditional IAM and other security best practices

Reference Architecture for Single Agent System

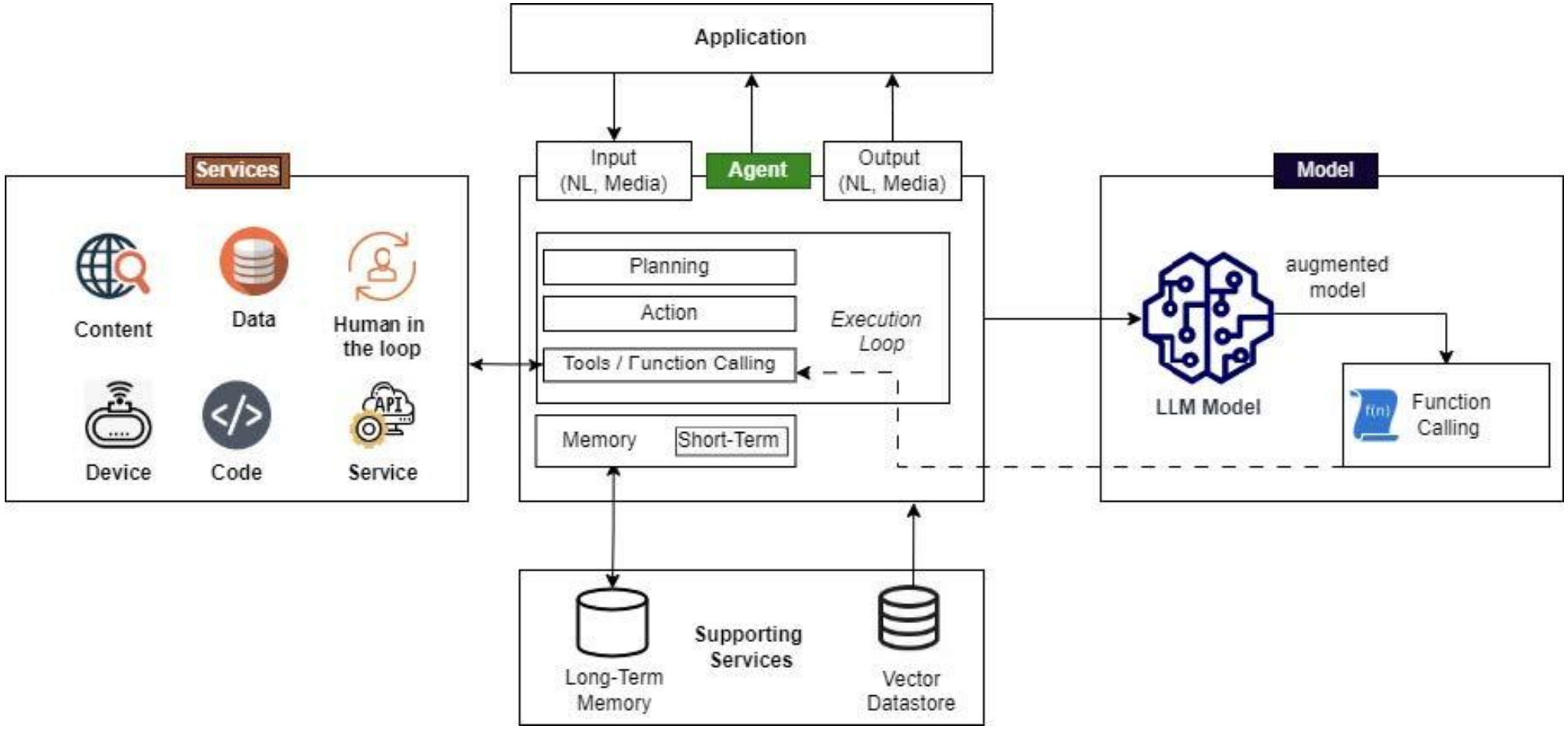

Image source: OWASP Foundation (owasp.org) - OWASP Agentic AI - Threats and Mitigation Guide

Reference Architecture for Multi Agent System

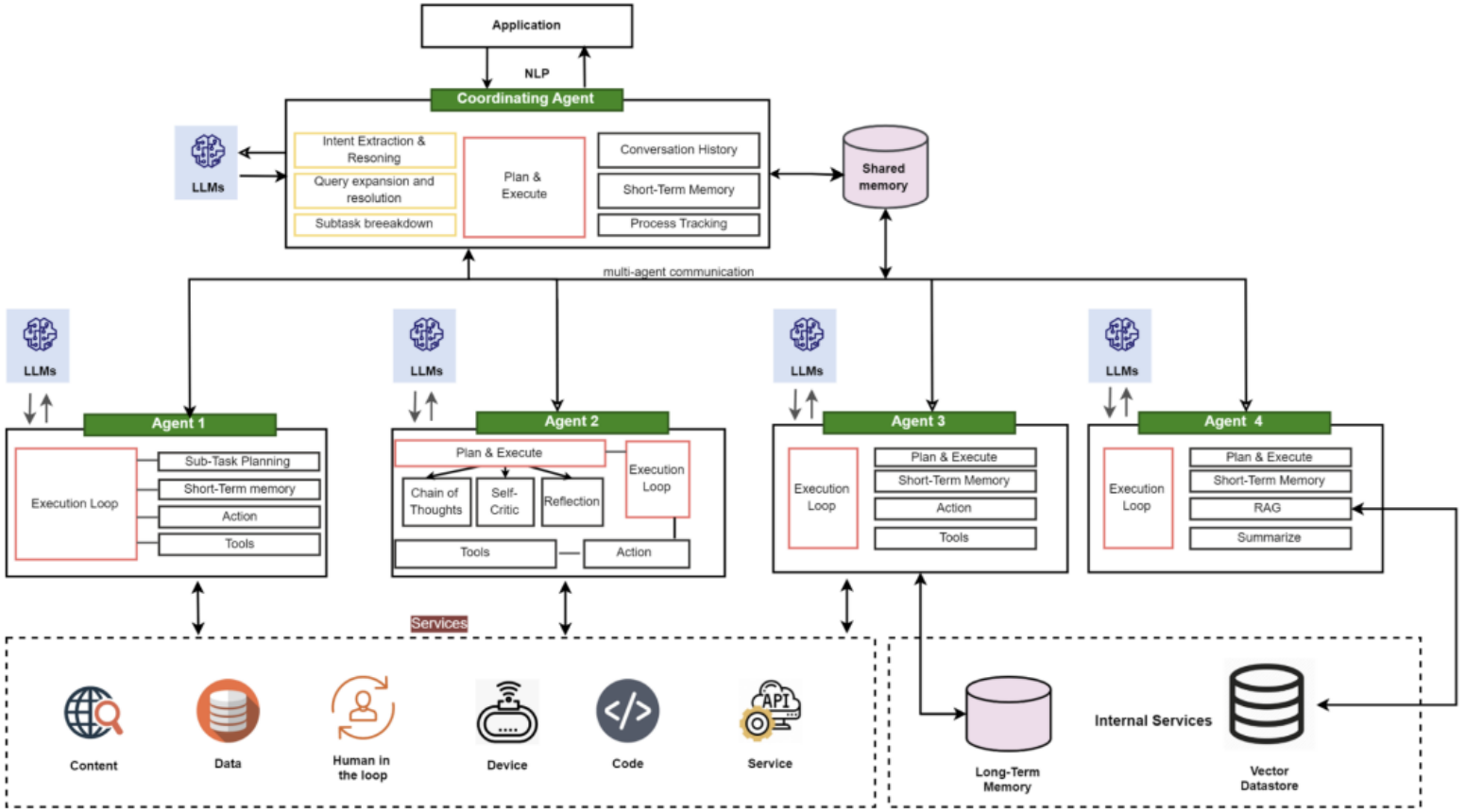

Image source: OWASP Foundation (owasp.org) - OWASP Agentic AI - Threats and Mitigation Guide

Resource List

- https://genai.owasp.org/resources/
- https://www.coalitionforsecureai.org/resources/

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Summit 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!