

Group Discussion A: Agentic AI to Empower OSPOs

Date: 27 July 2026, Sony Office Tokyo

Introduction

The session opened with an introduction presenting the objectives of the TODO Group's Agentic AI Working Group.

Reference: <https://github.com/todogroup/working-groups/blob/main/wg-agentic-ai/meeting-notes.md>

Proposed Discussion Topics

Several potential focus areas for the working group:

1. Compliance challenges in the AI era
2. Why permissive licenses are no longer sufficient
3. Open source AI: opportunities and risks
4. How Agentic AI changes open source strategy

Group Discussion

How to handle AI-Generated Code in Open Source Repositories?

The group discussed the growing challenges of AI-generated code in open source projects.

Key discussion points included:

- Existing open source software licenses may no longer adequately address AI-generated content.
- Traditional attribution models were designed for human authorship rather than AI-generated or AI-regenerated code.
- Under current U.S. copyright law, purely AI-generated works generally cannot be copyrighted, raising new questions for open source governance.
- Software licensing frameworks do not map cleanly to AI models and generated outputs.
- The Linux Foundation recently introduced the **OpenMDW License** to address licensing for machine learning models:
<https://openmdw.ai/>
- The **Agentic AI Foundation** and its **AgentGateway** project were also mentioned as emerging initiatives in this space.

Beyond the Model: An AI model Harness

The discussion emphasized that governing AI requires looking beyond foundation models alone. Important layers include:

- Instructions and context
- Tools

- Memory and state
- Execution loop
- Permissions
- Policy enforcement
- Observability

These layers collectively determine how AI agents behave and therefore become important governance considerations.

OSPOs and AI Governance

Participants discussed the evolving role of Open Source Program Offices (OSPOs) in the age of Agentic AI.

Questions raised included:

- What role should OSPOs play in governing AI infrastructure?
- Should responsibility instead reside with AI engineering teams or platform/infrastructure teams?
- How should organizations distinguish between:
 - governing AI systems, and
 - using AI to improve governance processes?
- Vendor management remains an important responsibility for many OSPOs, particularly as organizations adopt AI platforms and services.

Current Focus Areas of the existing Agentic AI Working Group

The working group is currently exploring topics such as:

- Scaling OSPO operations with AI
- AI governance and policy questions
- Demonstrations around AI authorship and provenance

Future Collaboration

Participants discussed whether there is sufficient interest within the Asia-Pacific open source community to establish an APAC-focused Agentic AI Working Group.

AI Transparency in Open Source Projects

Additional ideas discussed included:

- Creating AI-specific announcement templates for projects such as the Linux kernel and Kubernetes.
- Whether open source projects should introduce dedicated labels or disclosure mechanisms indicating when AI has been used to generate or substantially assist contributions.