intel

SFScon

7 November 2025

Navigating the AI Jungle

The OSPO's New Mandate for AI Governance

Alexios Zavras
Chief Open Source Compliance Officer

The AI Revolution is Here

Generative AI Adoption at Breakneck Speed

- Organizations rapidly deploying AI/ML models across all business functions
- ChatGPT, GitHub Copilot, and custom AI solutions becoming standard tools
- Traditional software governance frameworks struggling to keep pace
- The result: A significant governance black hole

Traditional OSPO Responsibilities

What OSPOs Have Mastered

- Open source license compliance and risk management
- Managing software dependencies and supply chain security
- Facilitating open source contributions and community engagement
- Vulnerability scanning and remediation processes
- Software Bill of Materials (SBOM) generation and maintenance
- Policy development and developer education

The Fundamental Shift

AI Has Redefined What a Software Asset Is

- Traditional view: Source code, binaries, libraries, dependencies
- New reality: Models, datasets, training pipelines, inference engines
- Software assets now include:
  - Pre-trained models and fine-tuned variants
  - Training and validation datasets
  - Model weights and parameters
  - AI-generated code and content

The AI Governance Gap

Why Traditional Tools Fall Short

- License scanners can't analyze model licensing terms
- Dependency trackers miss model provenance and lineage
- Security tools don't detect model-specific vulnerabilities
- SBOMs don't capture AI components and their relationships
- OSPOs are flying blind in the AI landscape

Challenge #1 — AI Licensing Complexity

Beyond Traditional Software Licenses

- Models often have custom licensing terms (e.g., "Responsible AI" clauses)
- Dataset licensing separate from model licensing
- Commercial use restrictions and attribution requirements
- License compatibility between models, datasets, and traditional software
- Action needed: Expand license compliance frameworks for AI assets

Challenge #2 — AI-Specific Vulnerabilities

New Attack Vectors and Risk Categories

- Model poisoning and adversarial attacks
- Data leakage and privacy violations
- Bias and fairness issues
- Prompt injection and jailbreaking
- Model inversion and extraction attacks
- Traditional vulnerability scanners miss these entirely

Challenge #3 — AI Supply Chain Complexity

Tracking AI Dependencies and Provenance

- Models built on other models (foundation → fine-tuned → specialized)
- Dataset provenance and quality concerns
- Training infrastructure and compute dependencies
- Third-party AI services and APIs
- Challenge: Creating comprehensive AI supply chain visibility

Challenge #4 — Evolving SBOMs for AI

Software Bill of Materials Must Include AI Components

- Traditional SBOMs: packages, versions, licenses, vulnerabilities
- AI-enhanced SBOMs need:
  - Model names, versions, and architectures
  - Training dataset information and sources
  - Model performance metrics and limitations
  - Inference dependencies and hardware requirements
  - AI service provider information

Challenge #5 — AI-Generated Code Governance

Managing Code Created by AI Systems

- Intellectual property and licensing questions
- Code quality and security concerns
- Attribution and liability issues
- Integration with existing code review processes
- Who owns AI-generated code? How do we audit it?

The Path Forward: OSPO Evolution

Expanding OSPO Capabilities for AI Governance

- Develop AI-specific policies and procedures
- Implement AI asset discovery and inventory tools
- Create AI risk assessment frameworks
- Establish AI model lifecycle management processes
- Build cross-functional partnerships (Legal, Security, Data Science)

Practical Next Steps

Building AI Governance Capabilities

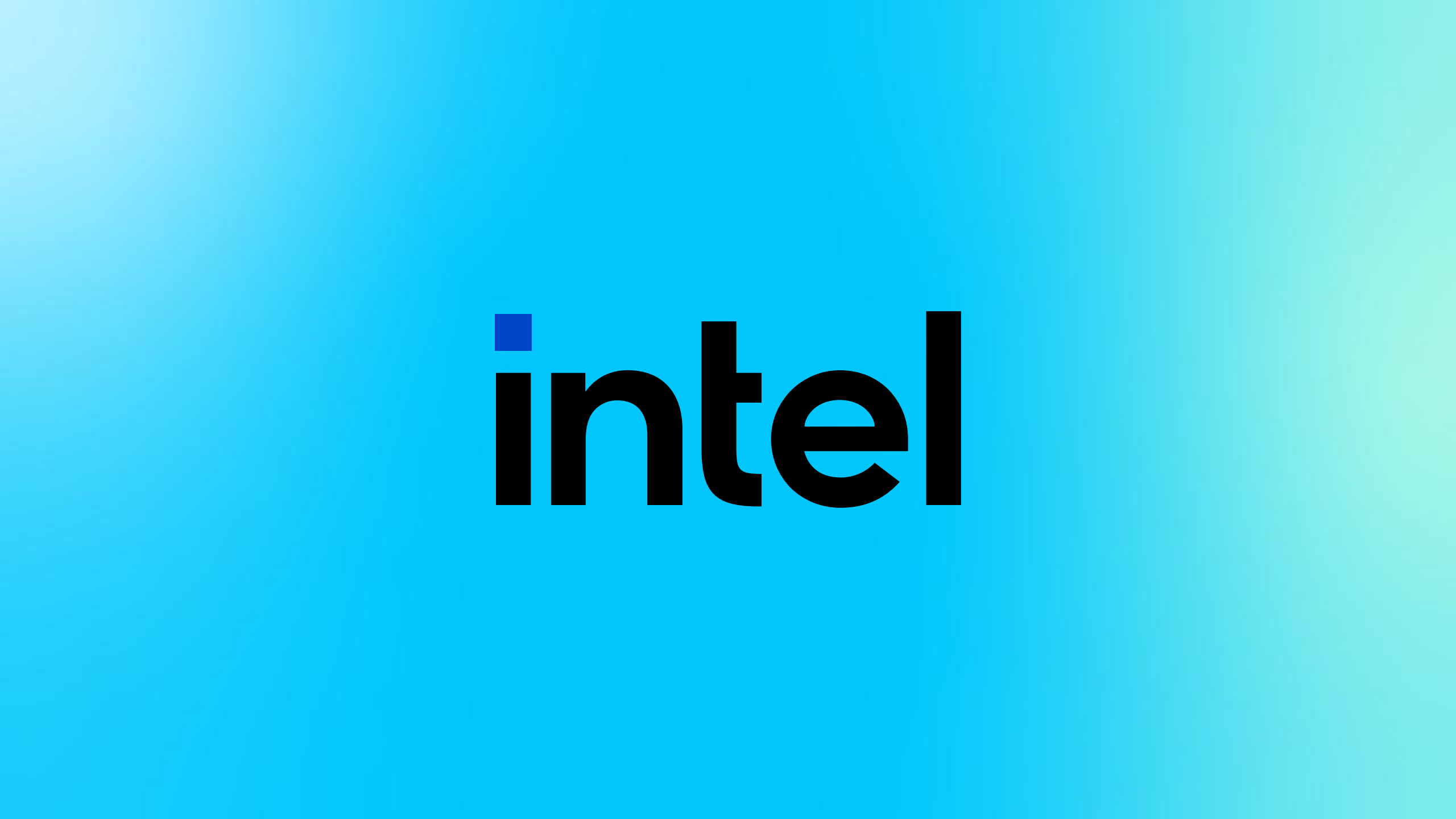
- Immediate: Inventory current AI usage across the organization
- Short-term: Develop AI-specific licensing and security policies
- Medium-term: Implement AI-aware SBOM and dependency tracking
- Long-term: Integrate AI governance into existing OSPO workflows
- Ongoing: Stay current with evolving AI regulations and standards

Conclusion

The Future of OSPO in an AI World

- AI governance is not optional — it's essential for organizational risk management
- OSPOs are uniquely positioned to lead AI governance initiatives
- Success requires expanding beyond traditional software management
- The time to act is now — before the governance gap becomes a crisis


intel


intel