

Open Source Standard

Lessons learned from establishing a governed enterprise capability

Published Nov, 2026



Meet the speaker

A practitioner’s perspective on building open-source governance in a regulated enterprise



Hari Vattappilli MBA • PMP

Open Source Enabler | Technology & Innovation Leader

What I bring to the conversation

Enterprise governance	Helping establish the Open-Source Program Office, including the enterprise Standard and supporting control procedures.
Transformation at scale	20+ years across financial services and technology, aligning cross-functional teams and executive stakeholders.
Innovation with measurable outcomes	Experience building business cases, modernizing operating models and translating emerging technology into practical adoption.

Career perspective

Dev foundation → QA CoE & program leadership → Infrastructure & innovation → OSPO enablement

Beyond the Professional Role

Painting, theatre, music, and others… my creative side













What the journey taught us

The Standard converts six practical lessons into enterprise controls

1. **Governance must keep pace**
2. **Adapt proven practices**
3. **Enable innovation safely**
4. **Can't manage what you can't see**
5. **Supply chains are broader**
6. **AI and OSS are connected**

Outcome: a risk-based framework that supports responsible innovation

Lesson 1: Governance must keep pace

Open source moved from a development choice to foundational enterprise infrastructure

1

What we observed

- Open source is embedded across applications, cloud platforms, AI and digital delivery.
- Requirements were dispersed rather than consolidated in a dedicated enterprise Standard.
- Internal conversations highlighted the material governance gap.

Key lesson

Foundational technology requires clear ownership, controls and accountability.



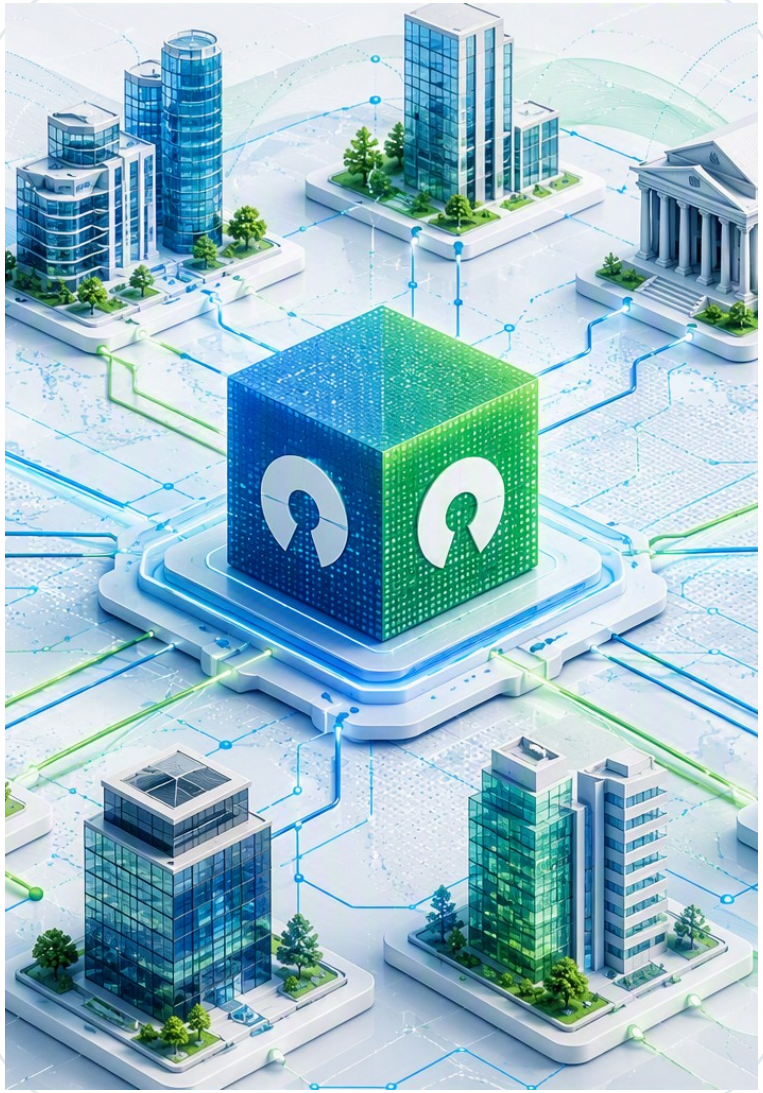
Lesson 2: Adapt proven practices

Benchmark externally, then tailor controls to TD's environment

2

- Reviewed practices from peer financial institutions and industry leaders.
- Referenced Fidelity Investments, The Linux Foundation and FINOS.
- Used established patterns to accelerate maturity and reduce implementation risk.

Do not reinvent mature governance. Learn, adapt and operationalize.



Lesson 3: Innovation and risk must advance together

The objective is controlled enablement, not restriction

3

Opportunity

Structured contribution can strengthen reuse, learning and workforce productivity.

Exposure

Unmanaged contributions can create legal, security, intellectual property and reputational risk.

Control response

External upstream contributions require governance approval and enterprise risk-mitigation processes.



Lesson 4: Visibility comes before governance

Risk decisions depend on knowing what is used, where it is used and under what terms

4

Approve Review software and dependencies before use

Inventory Maintain a centralized TD-approved record

Retain Manage and retain applicable licence information

Connect Map applications to their open-source dependencies

Without reliable inventory and dependency data, risk management remains reactive.



Lesson 5: The supply chain is broader than software

Modern delivery includes software, AI and cryptographic components

5

Monitor before deployment

- Establish enterprise capabilities to monitor open-source Bills of Materials.
- Assess software, AI and crypto components for risk before deployment.
- Block or slowdown deployment when open-source software or dependencies are not approved.

Shift from reactive discovery to preventive supply-chain control.



Lesson 6: AI governance and open source governance are connected

Open-source code, training data and model weights can create material AI risk

6

What changed

- AI systems frequently rely on open-source frameworks and components.
- AI risk assessments must consider open-source code, training data and weights.
- OSPO review is required to help identify material open-source risks.
- Governance must scale at the same pace as AI innovation. Leveraging AI tools and policy-as-code is essential.

Open source governance is a core pillar of responsible AI delivery.



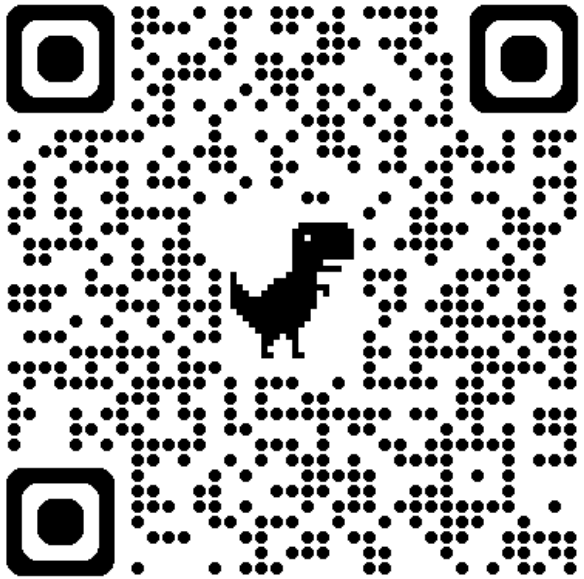
How the lessons translated into control requirements

Nine requirements establish the governance foundation

Use & inventory	Contribute	Monitor & trust	AI
• Approval before use • Centralized inventory • Licence management and retention • Application-to-dependency relationships	• Approval for external upstream contribution • Enterprise risk-mitigation processes	• BOM monitoring and deployment blocking • Trust registry for strategic projects	• OSPO review within AI risk assessments

Call to action

GitHub



FINOS



TODO Group



Thank you. Welcome Feedbacks

Focus stakeholder attention on contribution, inventory, monitoring and AI review

Creating an Enterprise Open Source Standard in a Regulated Financial Institution: Lessons Learned