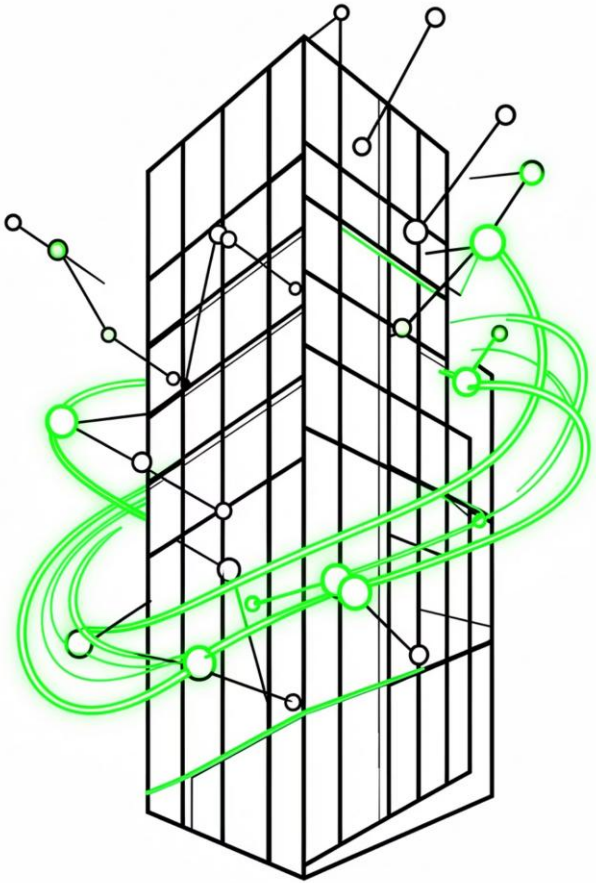
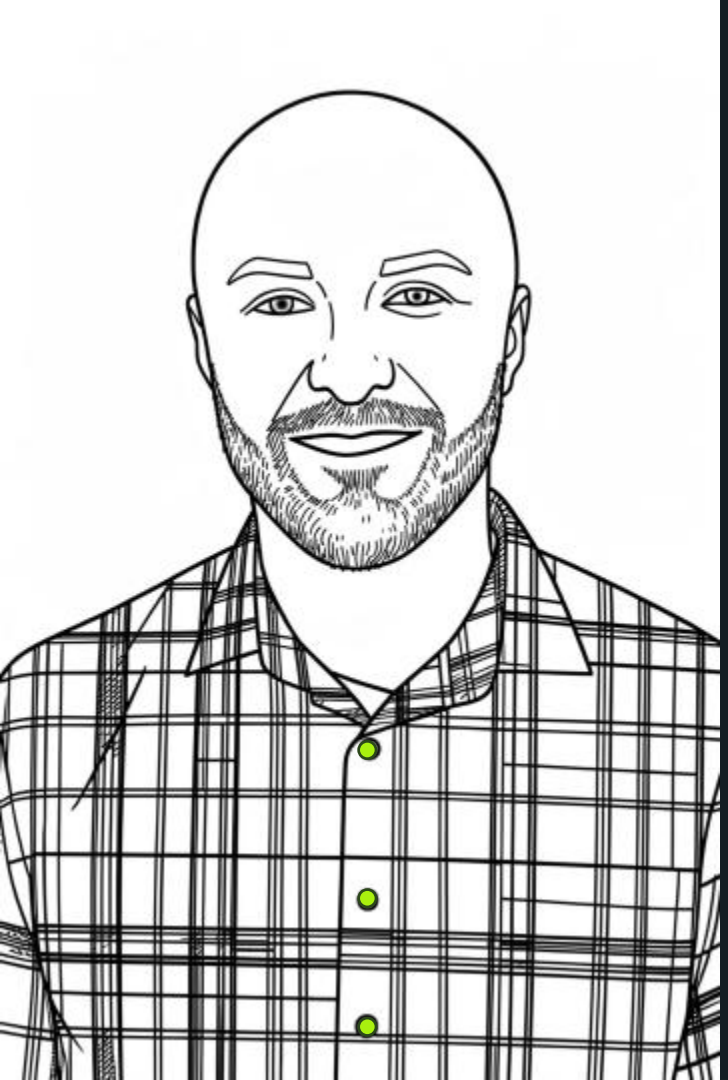


Architecting Secure Open Source Contributions in the Enterprise

The Git-Proxy Approach — A framework for controlled, compliant, and scalable OSS contribution

TOMASZ ŚWIERSZCZ · CITI



About Me

Tomasz Świerszcz

SVP Cloud Security Engineering · IT Architect · Founder

SVP Cloud Security Engineering at Citi

Leading cloud security engineering in financial services since 2024

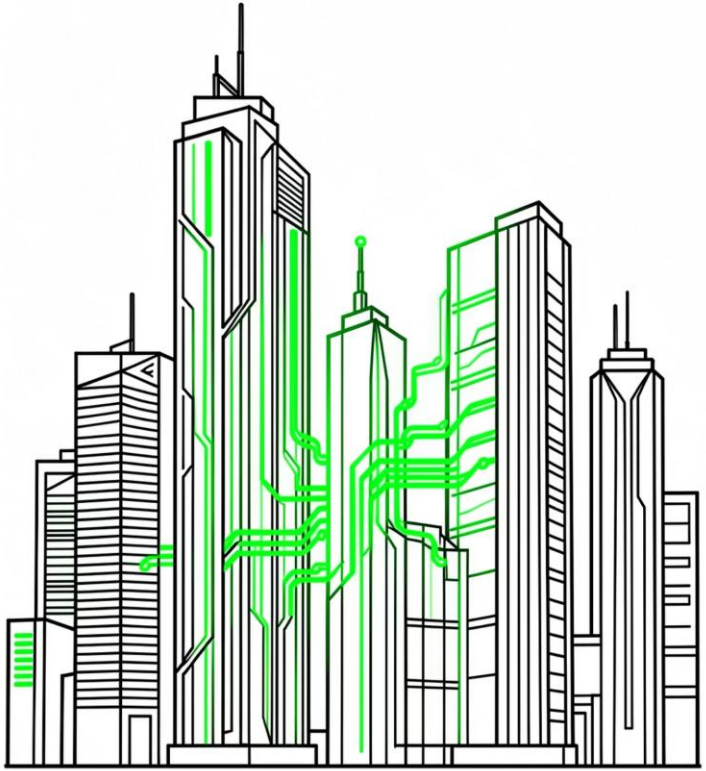
IT Architect & Software Engineer

21+ years of experience in system architecture, microservices, SOA, and software supply chain security

Founder of LAF Institute & Author

Author of LAF — a pragmatic guide to building effective IT architecture

I bridge hands-on software engineering with architecture and security to create practical, secure, and scalable technology solutions. Based in Warsaw, Poland.



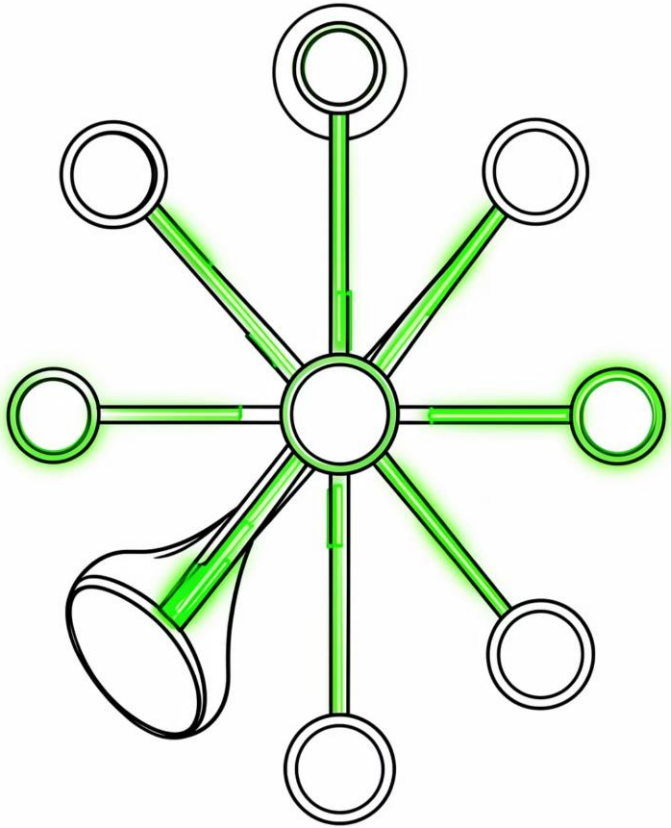
Why This Matters

Open source is no longer just developer tooling..

Organizations rely on open source to:

- accelerate software delivery
- reduce platform costs
- drive innovation
- build cloud-native systems
- participate in industry ecosystems

As enterprise dependency on OSS grows, governance and ecosystem stewardship become business-critical capabilities.



Why This Matters Now

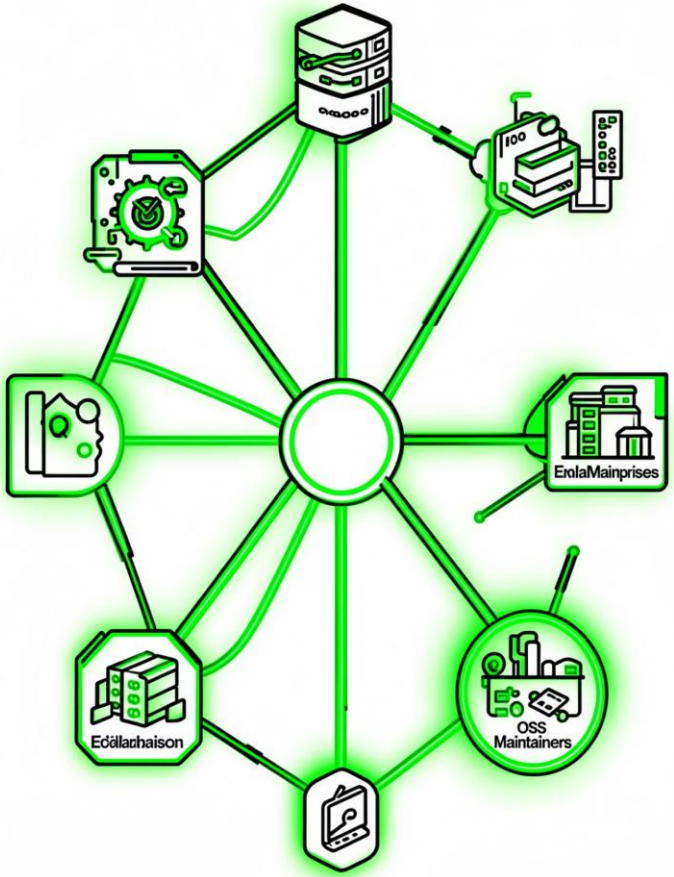
AI is accelerating software creation and upstream contributions.

At the same time:

- Open-source maintainers are overloaded
- Supply chain risks are increasing
- Security expectations are growing
- Enterprises need stronger governance

Open source is no longer just a dependency.

It must be a strategic relationship.



Why This Matters for the OSS Ecosystem

Open source maintainers are increasingly overloaded.

Meanwhile enterprises already operate:

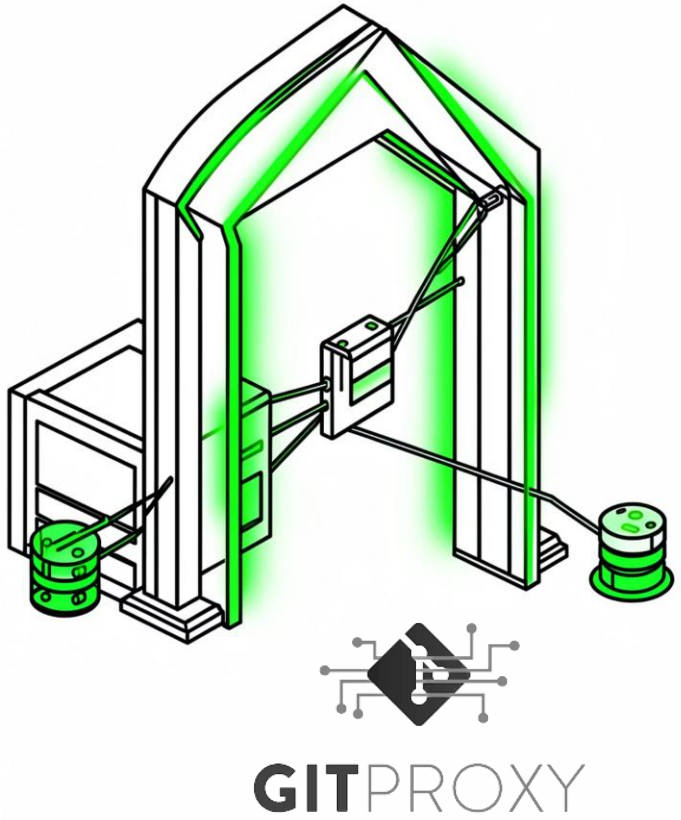
- Security tooling
- Policy engines
- Dependency intelligence
- AI-assisted analysis
- Supply chain controls

Git-proxy could help enterprises contribute governance intelligence back to the ecosystem.

What is Git-proxy?

GitProxy is an application that stands between developers and a Git remote endpoint (e.g., github.com). It applies rules and workflows (configurable as plugins) to all outgoing git push operations to ensure they are compliant.

The platform provides developers with clear remediation instructions directly in the terminal to minimize workflow disruption. It is especially useful for regulated industries like financial services, where companies need secure and auditable open-source contribution processes.



A Better Developer Experience

Compliance shouldn't slow engineers down. Git-Proxy is designed to get out of the way and let developers focus on what they do best.

Simple, Familiar Workflows

Git-Proxy works with standard `git push` commands. No new tools to learn, no process overhead.

CLI & IDE Integration

Native integration with popular development environments means feedback surfaces exactly where engineers work.

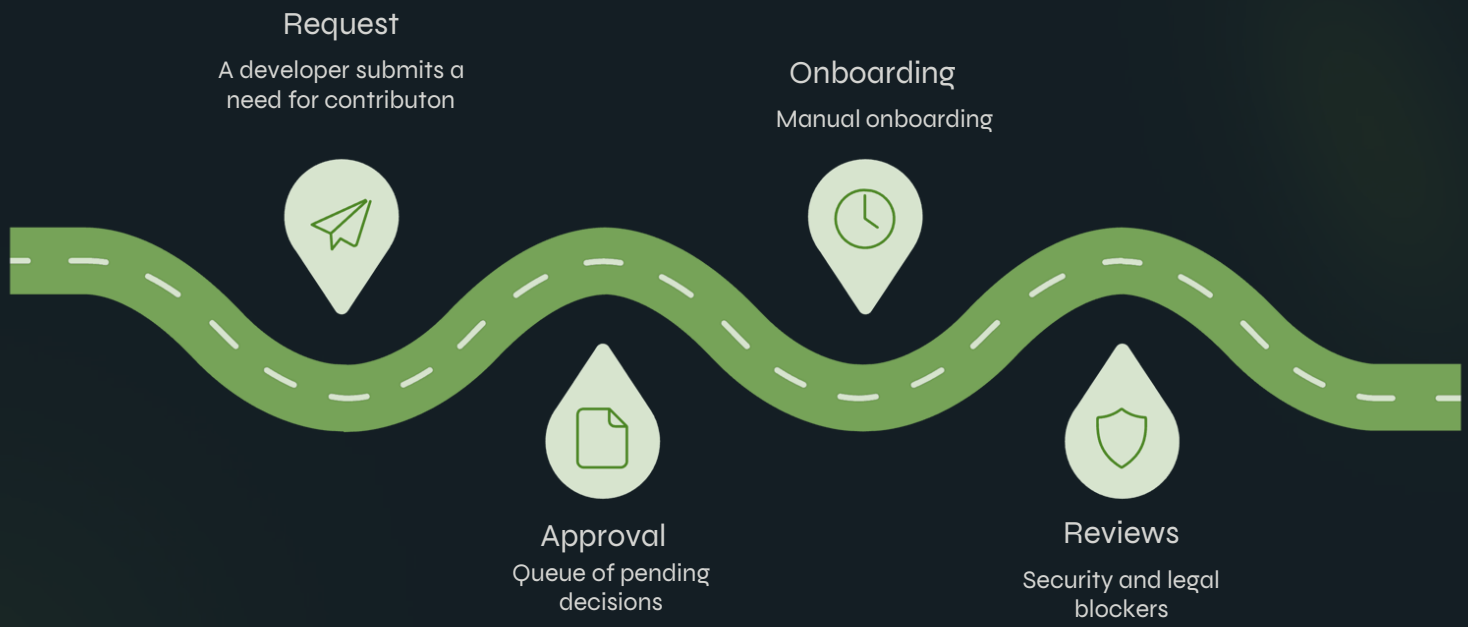
Instant Feedback

Policy violations surface in seconds — not days — giving developers clear, actionable guidance before a contribution stalls.

Demo

Enterprise Problem: Today's Contribution Flow

Manual management does not. scale The typical OSS contribution process in a large organization is a maze of manual approvals that frustrates developers and slows innovation.



Slow Feedback Loops

Weeks waiting for approval

Tool Fragmentation

Diffrent toosl than internal prcesses

High Operational Costs

Manual work multiplied across hundreds of projects

Process Bypassing

Frustrated developers bypass the rules

STRATEGIC PILLAR #0

The Shift: From Manual to Automated Governance

Enterprises are moving from manual, approval-heavy governance to policy-driven automation that embeds security and compliance directly into the development workflow.

From Manual to Policy-Driven

Policy-driven systems replace manual governance.

From Human to Automated

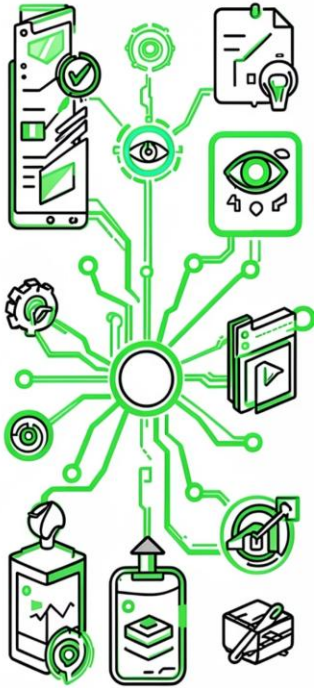
Automated enforcement replaces human approvals.

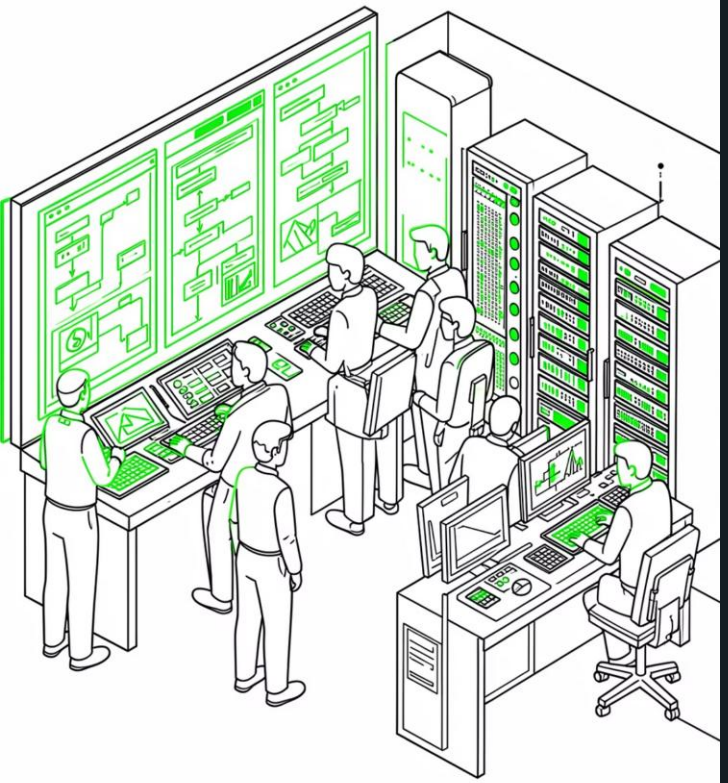
From Reactive to Embedded Security

Security is embedded in the workflow, not bolted on at the end.

From Periodic to Continuous Governance

Continuous compliance replaces reactive audits.L



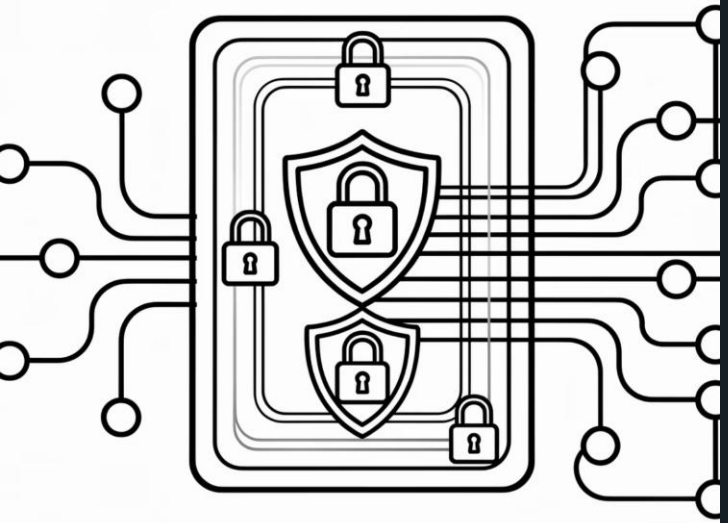


Strategic Pillar #1: Streamlining OSPO Operations

Git-proxy helps OSPO teams automate governance workflows:

- Automated onboarding
- Standardized workflows
- Contribution tracking
- Audit trails
- Workflow orchestration
- Reduced manual approvals

By own mechanism and integration with corportate tools



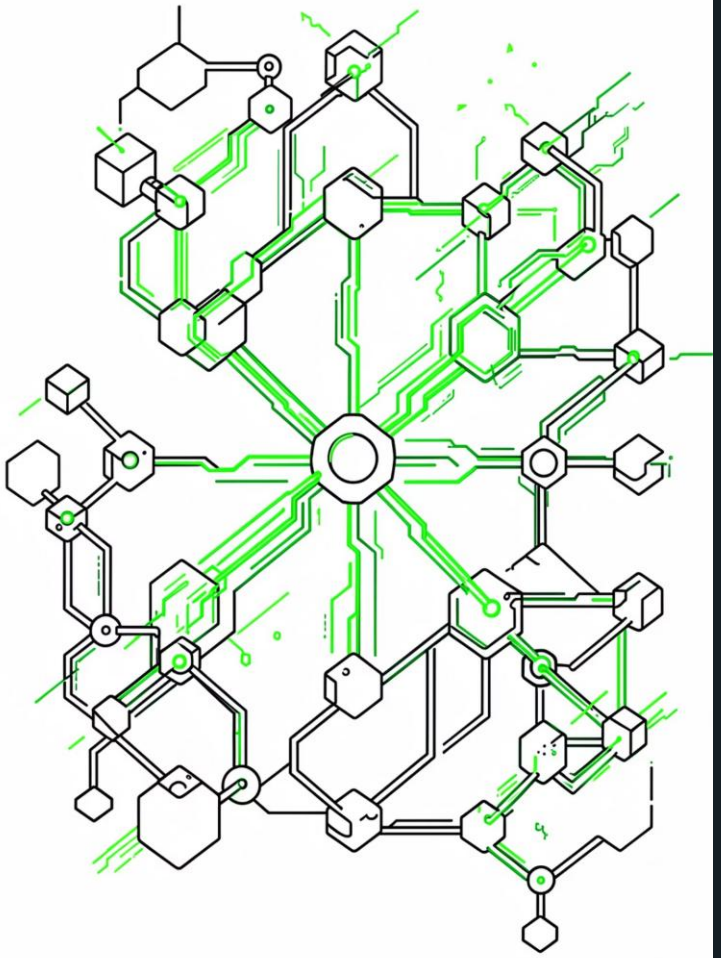
Strategic Pillar #2: Security & Compliance

Security becomes part of the workflow itself.

Git-proxy can enforce:

- Policy enforcement
- Compliance checks
- Security scanning
- License validation
- Supply chain controls

By own mechanism and integration with corportate tools



Beyond Contributions: OSS Decision Intelligence

Governance should begin at the onboarding stage. Git-proxy has the potential to evolve beyond contribution management — becoming an intelligence platform for all open source-related decisions in the organization.

OSS Onboarding Assessments

Automatic evaluation of each new open source project before adoption — eliminating manual reviews

Policy Fit Validation

Continuous verification of project alignment with evolving enterprise policies and requirements

Project Health Scoring

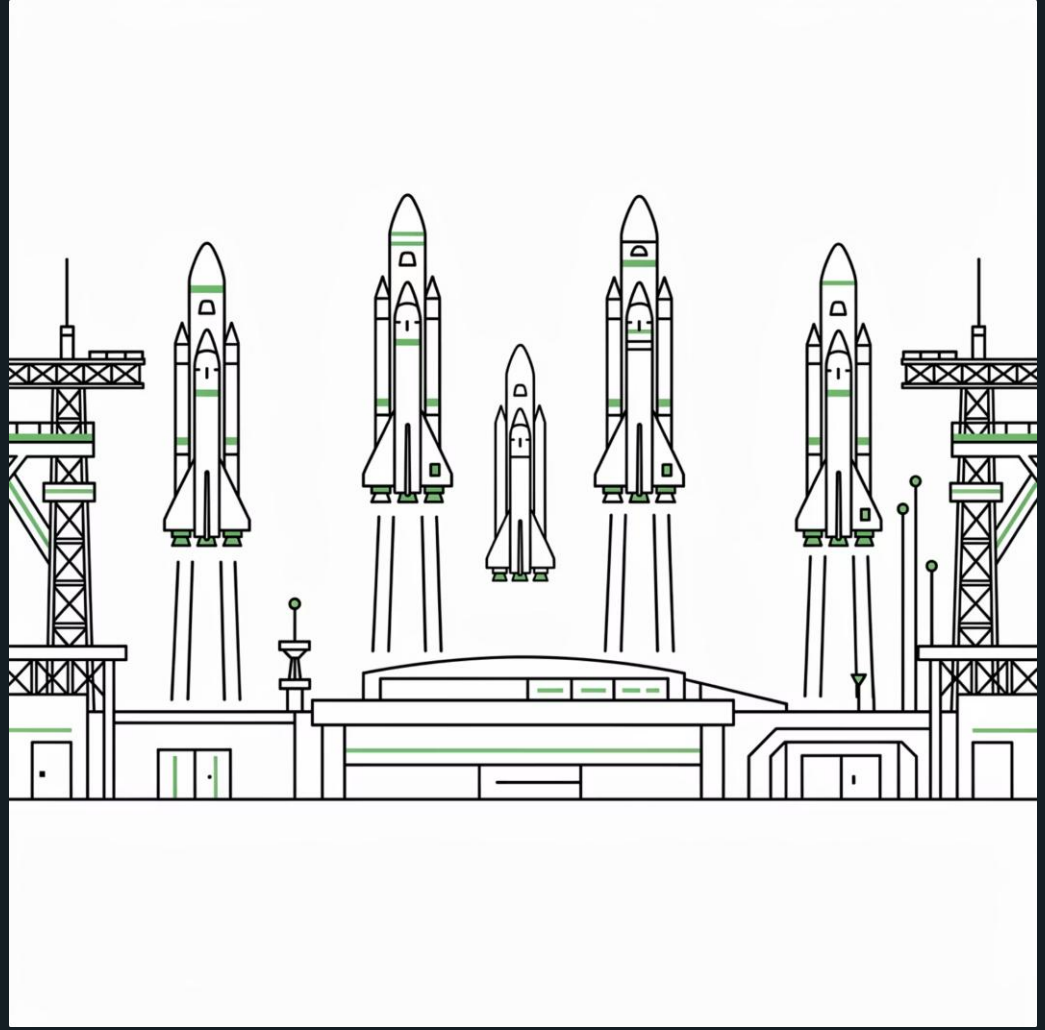
A quantifiable quality and risk indicator for every OSS project in the organization's portfolio

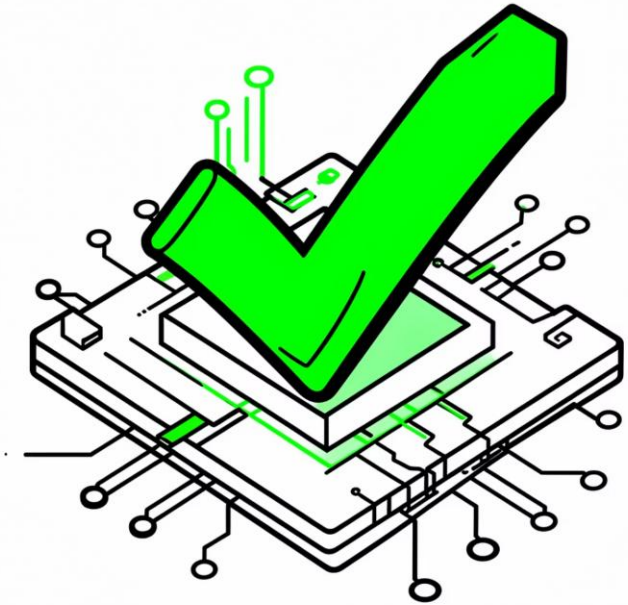
Supply Chain Risk Assessment

Proactive identification of threats in dependencies before they are exploited

OSS Project Onboarding Demo

GITPROXY





Approved Project Example

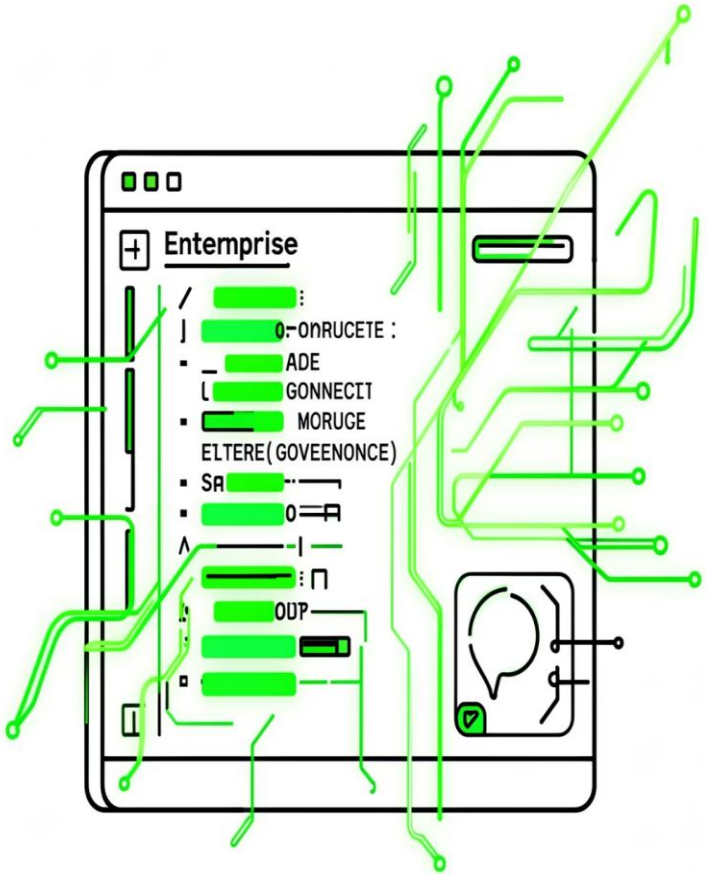
- License approved (Apache-2.0)
- Repository active
- Signed releases detected
- SECURITY.md present
- Policy fit approved

Governance Status: READY_FOR_ADOPTION

Blocked Project Example

- GPL-3.0 restricted
- Repository archived
- Maintainer activity low
- Strategic alignment failed

Governance Status: BLOCKED

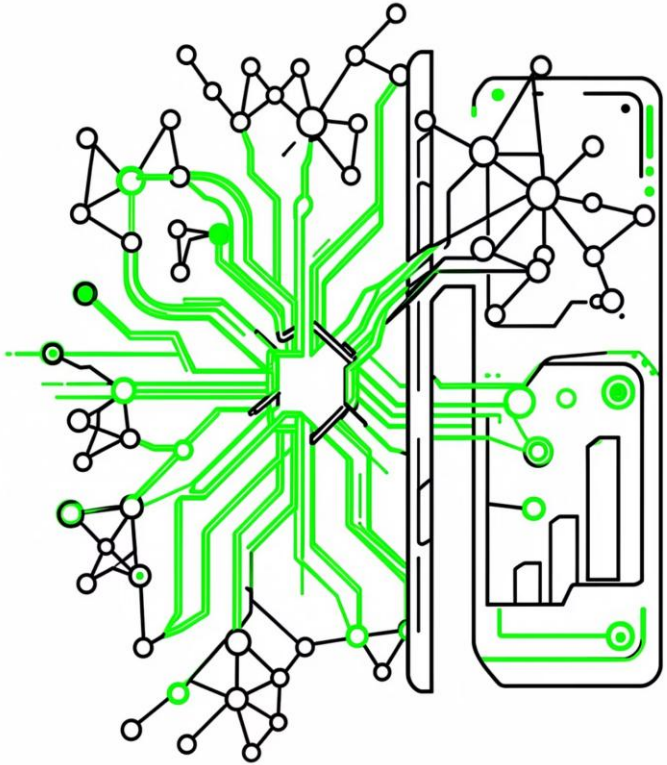


AI Assessment Demo

```
[Git-proxy] Running AI project quality assessment...

Documentation quality: GOOD
Maintainer responsiveness: MEDIUM
Bus factor risk: POSSIBLE
Enterprise fit: STRONG

AI Recommendation: APPROVE WITH OSPO REVIEW
```



Future Direction: AI-Assisted OSS Assessment

AI could help evaluate these items shown as icon+text:

- Documentation quality
- Maintainer responsiveness
- Project maturity
- Community health
- Enterprise fit

ORGANIZATIONAL IMPACT

Impact Across the Organization

OSPO

Lower operational overhead, better visibility, standardized governance

Developers

Faster workflows, better feedback loops, reduced friction

Security

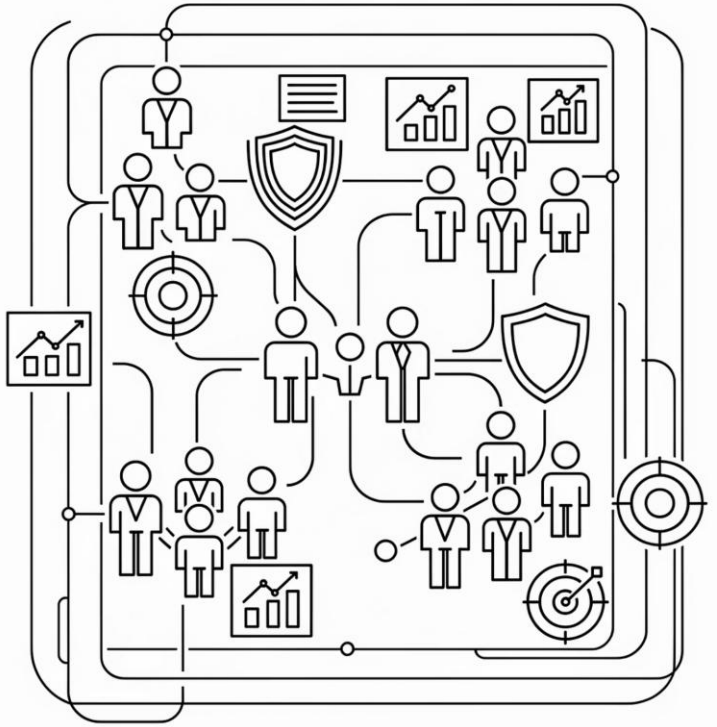
Earlier risk detection, better supply chain control, embedded compliance

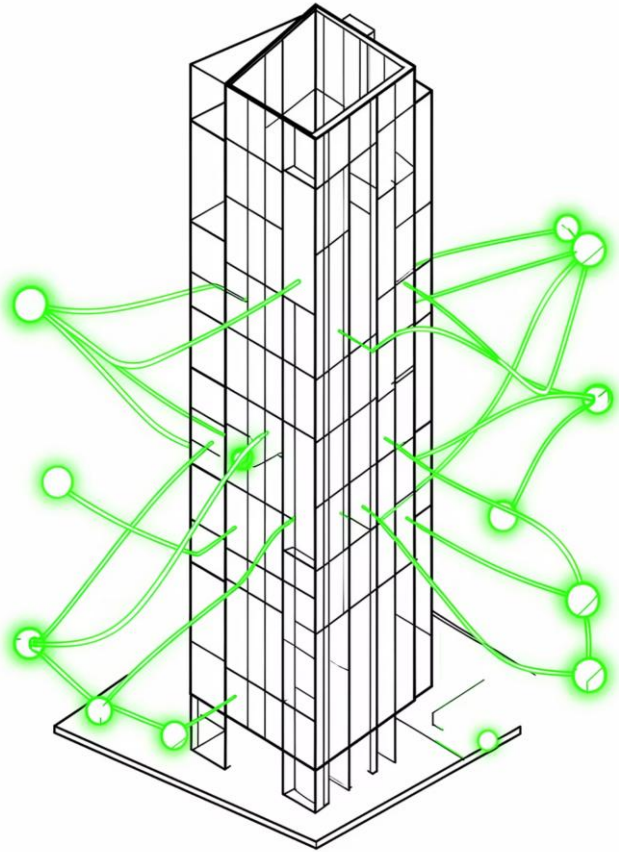
Enterprise

Scalable OSS governance, better strategic decisions

Key Takeaways

1. Automate governance
2. Embed security into workflows
3. Reduce developer friction
4. Start governance at onboarding
5. Use AI as an advisory layer





Q&A

https://git-proxy.finos.org/

TOMASZ ŚWIERSZCZ CITI

https://www.linkedin.com/in/tswierszcz mail@tomaszswierszcz.pl