FOSSID

Integrating Open Source Compliance in Your Internal Developer Platform Checklist

This checklist provides a practical framework for assessing and enhancing the integration of open source license compliance into your Internal Developer Platform (IDP). We recommend that organizations use this checklist to identify gaps, foster collaboration among OSPO, platform, compliance, legal, and security teams, and build a roadmap toward an automated, developer-friendly compliance program that supports both innovation and governance.

The checklist below is organized into key focus areas that collectively define a robust approach to embedding open source license compliance and security vulnerability checks into your IDP. Each area highlights a critical aspect of governance, ranging from policy integration and developer experience to pipeline automation and cross-functional collaboration, enabling organizations to assess their current practices and identify opportunities for improvement.

Evaluation of Results

If you're checking most of these checklist items as "Met", you've already transformed open source governance from a manual, reactive process into an automated, developer-friendly, and scalable system embedded within your IDP. This strong foundation enables your organization to meet growing expectations from customers, regulators, and internal stakeholders without slowing down innovation.

If, however, there are gaps, your organization may face hidden risks from AI-generated code, license drift, and untracked third-party dependencies, each of which can lead to operational, legal, and financial consequences over time.

We recommend using this checklist as a starting point to foster closer collaboration between your OSPO, platform, legal, and security teams. Together, you can build a roadmap toward a seamless and compliant developer platform that strikes the right balance between velocity and governance.

1. Policy Integration

Organizations need to have clear, enforceable open source and AI-related policies as the foundation of their open source license compliance efforts. This section evaluates whether the organization has defined and integrated these policies into developer workflows.

Checklist Items	Assessment	Improvement or Remediation
1.1 Are clear, open source compliance, and AI policies defined, including allowed/ prohibited licenses, use of AI-generated code, and snippet reuse risks?	☐ Met ☐ Partially ☐ Unmet	
1.2 Are these policies enforced programmatically as policy-as-code in CI/CD pipelines and deployment workflows?	☐ Met ☐ Partially ☐ Unmet	
1.3 Do policies explicitly address AI-related risks, such as snippet detection and data/model provenance?	☐ Met ☐ Partially ☐ Unmet	

2. Developer Experience Enablement

Open source license compliance is most effective when developers are empowered to act independently. This section examines how compliance visibility, tools, and remediation guidance are integrated into the developer experience.

Checklist Items	Assessment	Improvement or Remediation
2.1 Is compliance visibility surfaced in developer portals showing SBOMs, license obligations, and risk status per service?	☐ Met ☐ Partially ☐ Unmet	
2.2 Do developers have access to self-service tools (such as CLI and IDE plugins) that enable them to scan code for license violations, vulnerabilities, and snippet-level risks before merging code?	☐ Met ☐ Partially ☐ Unmet	
2.3 Is there a documented, easy-to-follow remediation workflow when license compliance violations or security vulnerabilities are detected?	☐ Met ☐ Partially ☐ Unmet	

3. CI/CD Pipeline Controls

CI/CD pipelines serve as critical control points in any development environment. This section discusses the integration of automated scans, gates, and SBOM generation into build and deployment processes.

Checklist Items	Assessment	Improvement or Remediation
3.1 Are Software Composition Analysis (SCA) tools integrated into all build pipelines?	☐ Met ☐ Partially ☐ Unmet	
3.2 Are SBOMs generated automatically during builds and stored alongside release artifacts?	☐ Met ☐ Partially ☐ Unmet	
3.3 Are there pre-merge and pre-release gates to block non-compliant licenses, known vulnerabilities (CVEs), and unapproved dependencies?	☐ Met ☐ Partially ☐ Unmet	
3.4 Has snippet detection been integrated into pipelines to identify and mitigate risks associated with AI-generated code and potential copyright infringement?	☐ Met ☐ Partially ☐ Unmet	

4. Artifact and Metadata Management

This section assesses how build artifacts and their associated SBOMs are versioned, stored, and enriched with searchable metadata in support of traceability and audit readiness.

Checklist Items	Assessment	Improvement or Remediation
4.1 Does every build artifact have an associated versioned SBOM?	☐ Met ☐ Partially ☐ Unmet	
4.2 Are SBOMs stored centrally (in an artifact repository or SBOM registry) with searchable metadata?	☐ Met ☐ Partially ☐ Unmet	
4.3 Can you trace the full provenance, including license history, package origin, and vulnerability status, of all components across all products and services?	☐ Met ☐ Partially ☐ Unmet	

5. Governance and Audit Readiness

This section examines whether dashboards, audit trails, and periodic reviews are in place to monitor compliance and respond to emerging security risks.

Checklist Items	Assessment	Improvement or Remediation
5.1 Is there a centralized compliance dashboard visible to OSPO, security, and legal that tracks license usage, vulnerabilities, and policy adherence?	☐ Met ☐ Partially ☐ Unmet	
5.2 Are audit trails automatically maintained for license compliance, SBOM generation, and enforcement actions?	☐ Met ☐ Partially ☐ Unmet	
5.3 Are SBOMs reviewed periodically to detect emerging risks, such as newly disclosed CVEs or changes in licenses?	☐ Met ☐ Partially ☐ Unmet	

6. AI-Specific Guardrails

AI-generated code introduces new risks. This section evaluates whether your organization has implemented safeguards, detection mechanisms, and training to manage these challenges.

Checklist Items	Assessment	Improvement or Remediation
6.1 Has the OSPO assessed developer use of AI coding assistants for potential license/ copyright risks?	☐ Met ☐ Partially ☐ Unmet	
6.2 Is snippet detection actively monitoring for code fragment reuse from AI-generated out-puts?	☐ Met ☐ Partially ☐ Unmet	
6.3 Did you provide training to developers about the risks and responsibilities of AI-generated code?	☐ Met ☐ Partially ☐ Unmet	

7. Cross-Functional Collaboration

Compliance is a shared responsibility across many departments within the organization. This section examines how well OSPO, platform engineering, security, compliance, and legal teams collaborate to embed and maintain compliance in the IDP.

Checklist Items	Assessment	Improvement or Remediation
7.1 Does the OSPO collaborate closely with platform engineering to embed compliance directly into the Internal Development Platform (IDP)?	☐ Met ☐ Partially ☐ Unmet	
7.2 Is there a standing relationship between OSPO, legal/IP, compliance, and security teams to jointly manage open source and AI risks?	☐ Met ☐ Partially ☐ Unmet	
7.3 Are platform teams empowered and supported to implement and maintain these compliance features?	☐ Met ☐ Partially ☐ Unmet	