


From Policy to Pipeline: How OSPOs Can Power Regulatory Readiness and Upstream Impact



Agenda

- About us
- Policy and Regulations:
 - India: SEBI CSCRF, CERT-In SBOM and CS Audit Guidelines
 - EU CRA, US executive order, other guidelines
- How OSPOs can help
 - Interpret and implement region-specific regulatory requirements
 - Collaboration between different teams in an organization
 - Participate and foster open standards and communities
 - Contribute and engage upstream for ecosystem wide readiness
- AboutCode: Live Demo
- Questions?

About Arun

- Head of Secure Development Lifecycle: Corporate Cybersecurity Technology at Siemens Healthineers
- Leading teams for Open Source Software License and Security Compliance for Medical Devices
- Links:
 - LinkedIn: <https://www.linkedin.com/in/arunazhakesan>

About Ayan and AboutCode

- Core maintainer of [ScanCode](#) (scancode-toolkit and scancode.io)
- Working on license detection, package identification, binary scanning, devel/deployed mapping, SBOMs and data summarization
- AboutCode's FOSS-first mission: FOSS for FOSS
 - Open source tools and open data (AboutCode stack)
 - Simple and practical standards (Package-URL)
 - Applications for Legal Business users (DejaCode, also FOSS)
- Links:
 - asmahapatra@aboutcode.org
 - GitHub: <https://github.com/AyanSinhaMahapatra/>
 - LinkedIn: <https://www.linkedin.com/in/ayansinhaju/>

Regulations readiness

- India
 - Cyber Security and Cyber Resilience Framework for SEBI Regulated Entities
 - Vulnerability disclosure, SBOMs
 - CERT-In guidelines:
 - Technical guidelines on SBOMs
 - Cyber Security Audit Policy Guidelines
- EU's Cyber Resilience Act (CRA)
- US Executive order 14028
- Global trend: regulators expecting detailed visibility into their software supply chains — and to prove it

OSPOs: Policy to Pipeline

- Requirements:
 - Generate and produce SBOMs
 - Vulnerability Disclosure
 - Secure development lifecycle
 - License Attribution
- MNCs: regulatory requirements are region specific
- Enable automation and policies

OSPOs: Policy to Pipeline

- Organizations have many stakeholders in FOSS
 - Product security
 - Legal and Compliance
 - Engineering teams
 - Business functions
- OSPOs can facilitate collaboration
- embed compliance into the development lifecycle

OSPOs: Policy to Pipeline

- Participation in open standards
 - Openchain
 - SBOM standards: SPDX, CycloneDx
- Cross-organisation collaboration
 - Tools and automation
 - Open data

OSPOs: Policy to Pipeline

- Contribute upstream!
 - Identify projects with risk/need for help
 - Help with development, maintenance, funds
- Cost-effective solutions: supporting FOSS vs buying products

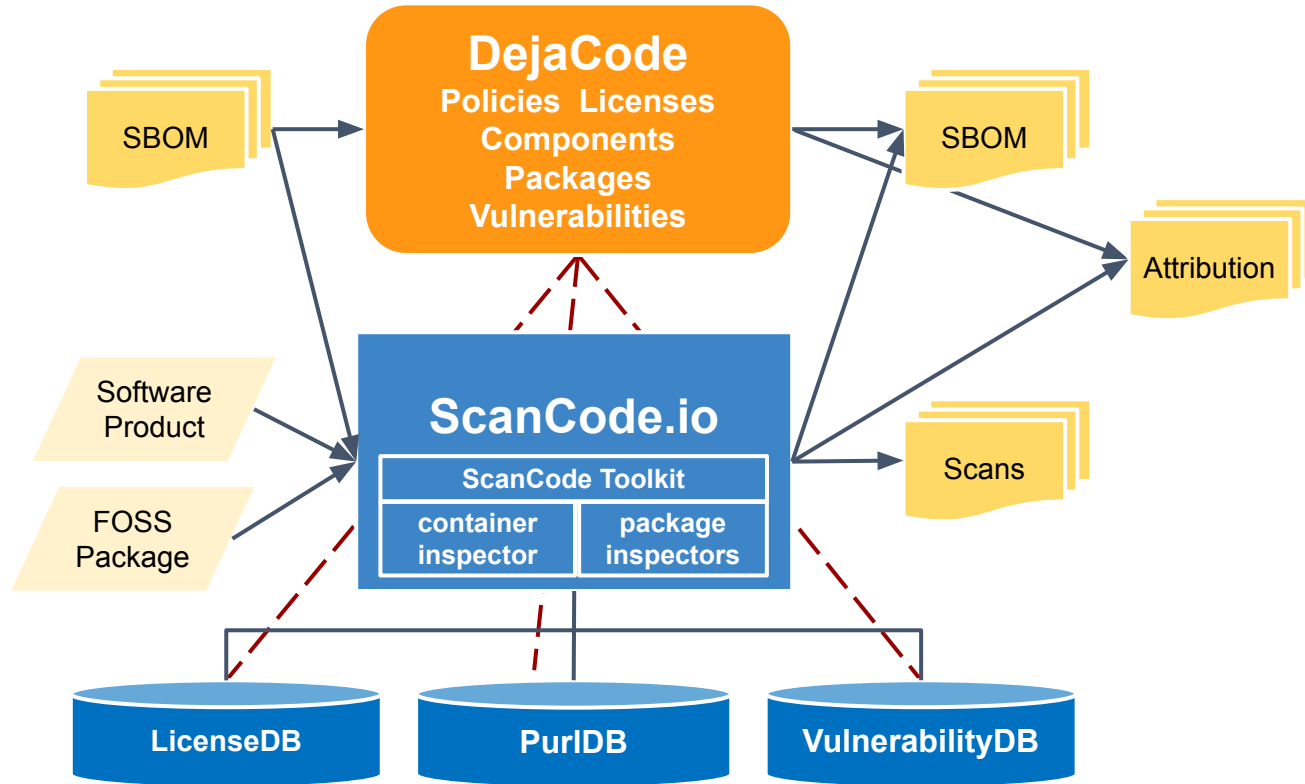
OSPOs: Policy to Pipeline

- [The Three Fs of Open Source Puppy Care](#): Michael Winsor
 - relationships with dependencies are important!
- Complete dependency graph
- Fix
 - Engage with maintainers, open Issues/PRs
- Fork
 - Maintain your version, apply patches
- Forget
 - Use something else!
- Fund!

Tools to empower OSPOs

- Enable automation and verification
- Embed into development lifecycle
 - (CIs) Continuous Integration
 - Flag licensing and security compliance issues
 - Risk analysis for all dependencies
 - Empower reusing FOSS safely
- Help with curation and oversight
- Help meet regulatory requirements
 - Generate SBOMs, Vulnerability Disclosure, License Attribution
- Map outputs to compliance artifacts required by regulators across regions

The AboutCode stack:



Why AboutCode?

- Non-profit, fully open source and open data
- options: CLI tool, Github action, web app, scans: containers, source/binary etc
- supports and working with package ecosystems
 - to build better metadata, more transparency
 - solve ecosystem wide problems at once
- Open data
 - Curated and open data on Licensing, Vulnerabilities, reuse scan results
- Large community
 - working with FOSS orgs to improve standards, data and transparency
 - OSPOs, Security, Lawyers, Specifications, Developers

Live Demo!

Other FOSS SCA tools and projects

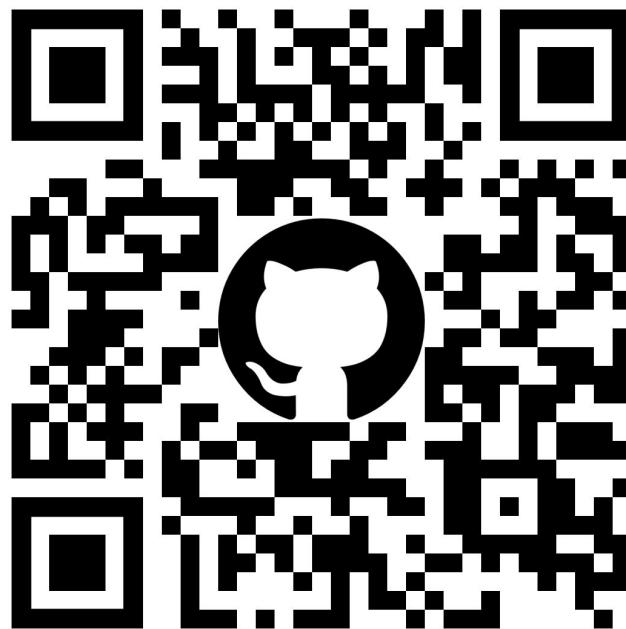
- [ORT: OSS Review Toolkit](#) (Uses ScanCode)
- [FOSSology](#) (Uses ScanCode)
- [SW360](#)
- [TERN](#) (Uses ScanCode)
- [ClearlyDefined](#) (Uses scancode)
- [OSSelot](#)
- OWASP [DependencyTrack](#)
- OWASP [DepScan](#)
- [AppThreat](#) projects: atom, chen, vdb
- CycloneDx [cdxgen](#)
- Anchore: [syft](#), [grype](#)
- Aquasec [trivy](#)

Questions?





Link to slides



[github/aboutcode-org](https://github.com/aboutcode-org)

Credits

Special thanks to all the people who made and released these excellent free resources:

- ▷ All the open source software authors that make AboutCode possible
- ▷ [xkcd](#) comics under [cc-by-nc-2.5](#)
- ▷ Presentation template by [SlidesCarnival](#)