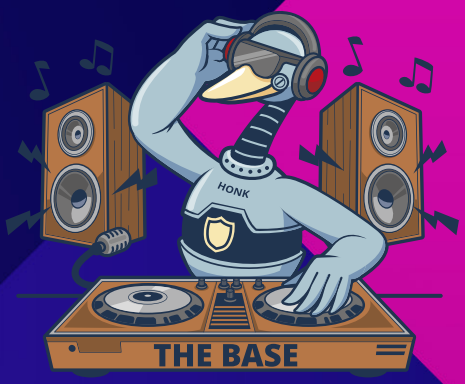
OpenSSF

OPEN SOURCE SECURITY FOUNDATION

OPEN SOURCE PROJECT SECURITY BASELINE

The **OpenSSF** community has produced this **control catalog** in collaboration with Linux Foundation partners — including **CNCF**, **FINOS**, and **OpenJS**. The **open source** project outlines best-practice security requirements aligned with industry standards and global regulations — all supported by tools for automation, evidence generation, and CI/CD policy enforcement.



Key Benefits

For Developers & Maintainers

- Clear, actionable guidance to improve security.
- Demonstrates commitment to secure development practices.
- Reduces repetitive security requests from downstream consumers.

For Consumers & Organizations

- Transparent, verifiable evidence of upstream project security.
- Streamlines compliance with global standards (e.g., CRA, NIST SSDF).
- Enables due diligence and risk management practices.

The Baseline Framework

The OSPS Baseline defines **41 security requirements** across **three maturity levels**, structured within six lifecycle stages. Each stage is supported by documentation, automation, and reporting to help projects demonstrate security practices at scale.

Sample: OSPS-AC-3.01

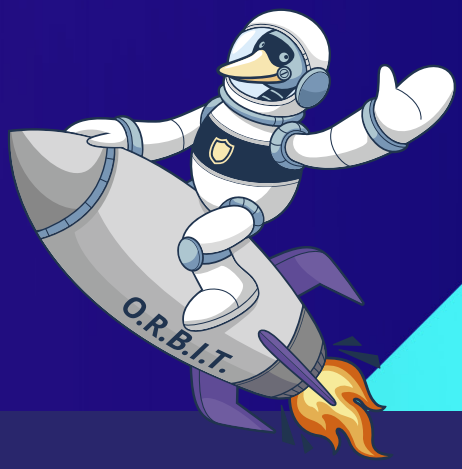
When a direct commit is attempted on the project's primary branch, an enforcement mechanism MUST prevent the change from being applied.

Supporting Tools and Ecosystem Projects

The **ORBIT Working Group** helps drive coordination, interoperability, and sustainability of projects across the open source security ecosystem.

- Security Insights, OSPS Baseline, OSPS Assessments
- OpenSSF Scorecard, Best Practices Badges, Darn/Darnit
- Minder, Ampel, Privateer, Gemara

Chat with ORBIT on Slack!



HOW TO PARTICIPATE IN THE OPENSSF

openssf.org

openssf.slack.com

github.com/ossf

linkedin.com/company/openssf