OpenSSF Security Baseline

Best Practices for projects to follow and downstream to seek out

Eddie & CRob, June 2025 - OCD

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

What is the Baseline?

Est. 2024

The OpenSSF's Open Source Project Security Baseline (OSPS Baseline or simply "Baseline") refers to a collection of efforts led by the OpenSSF in collaboration with members and LF partners (CNCF, FINOS, OpenJS).

The Baseline includes a **Catalog** of requirements that map to industry standards, frameworks, and regulations, and **Tooling** to assist in determining Baseline-compliance, that automate Baseline configuration settings, and links to evidence and attestations.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

All your Base are belong to us

OpenSSF Announces Initial Release of the Open Source Project Security Baseline

How to Use Open Source Project Security Baseline to Better Navigate Standards & Regulations?

Tech Talk | Thur. April 24, 2PM ET

The OpenSSF Security Baseline was officially released Feb 2025

Based on a library of well-known cybersecurity frameworks, standards, and global regulations

It includes 40 requirements across 3 levels of maturity covering 8 areas of cyber and application security practices

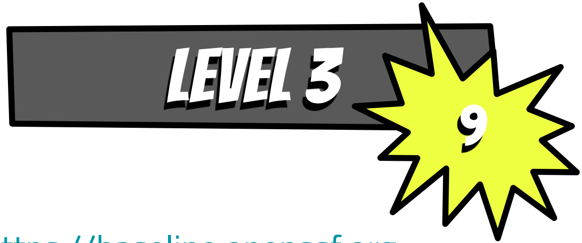
- Access Control
- Build & Release
- Documentation
- Governance
- Legal
- Quality
- Security Assessment
- Vulnerability Management

https://baseline.openssf.org
https://github.com/ossf/security-baseline
https://github.com/ossf/wg-ORBIT

What are these levels you speak of?

- “Universal security floor” for all open source - great for single maintainer or early maturity projects
  - Are you a Foundation? the level 1 baseline should be your first set of criteria for maturing projects (or even accepting projects).

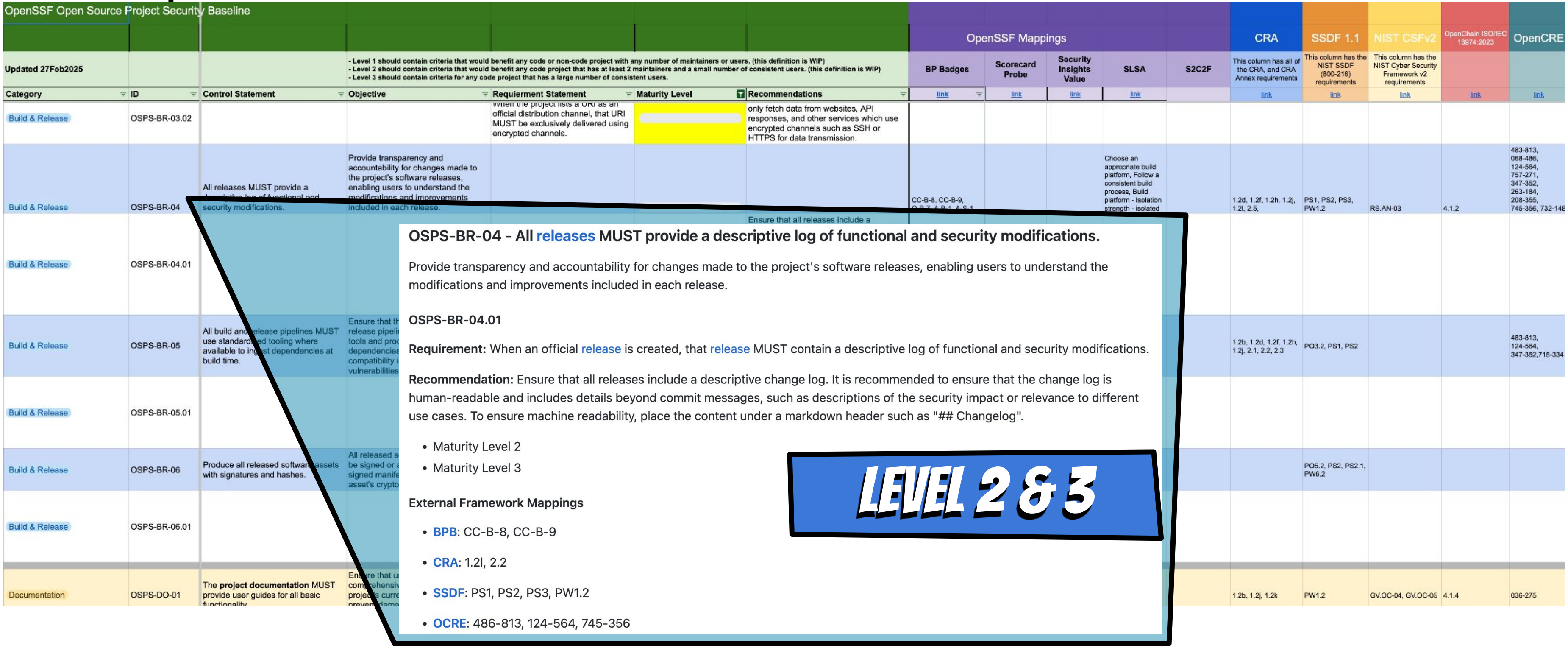
- “Let me get my cli, I got this” - good for projects with 2 - 6 maintainers and maturing



- Security *flex* - good for highly mature projects that consider security a core competency
  - Are you in a Foundation with project resources? You should strive for this one.

https://baseline.openssf.org
https://github.com/ossf/security-baseline

Compliance Crosswalk



OpenSSF Open Source Project Security Baseline							OpenSSF Mappings					CRA	SSDF 1.1	NIST CSFv2	OpenChain ISO/IEC 18974:2023	OpenCRE
Updated 27Feb2025			- Level 1 should contain criteria that would benefit any code or non-code project with any number of maintainers or users. (this definition is WIP) - Level 2 should contain criteria that would benefit any code project that has at least 2 maintainers and a small number of consistent users. (this definition is WIP) - Level 3 should contain criteria for any code project that has a large number of consistent users.				BP Badges	Scorecard Probe	Security Insights Value	SLSA	S2C2F	This column has all of the CRA, and CRA Annex requirements	This column has the NIST SSDF (800-218) requirements	This column has the NIST Cyber Security Framework v2 requirements		
Category	ID	Control Statement	Objective	Requierment Statement	Maturity Level	Recommendations	link	link	link	link		link	link	link	link	link
Build & Release	OSPS-BR-03.02			When the project lists a URI as an official distribution channel, that URI MUST be exclusively delivered using encrypted channels.		only fetch data from websites, API responses, and other services which use encrypted channels such as SSH or HTTPS for data transmission.										
Build & Release	OSPS-BR-04	All releases MUST provide a descriptive log of functional and security modifications.	Provide transparency and accountability for changes made to the project's software releases, enabling users to understand the modifications and improvements included in each release.				CC-B-8, CC-B-9,			Choose an appropriate build platform, Follow a consistent build process, Build platform - Isolation strength - isolated		1.2d, 1.2f, 1.2h, 1.2j, 1.2l, 2.5,	PS1, PS2, PS3, PW1.2	RS.AN-03	4.1.2	483-813, 068-486, 124-564, 757-271, 347-352, 263-184, 208-355, 745-356, 732-148
Build & Release	OSPS-BR-04.01					Ensure that all releases include a										
Build & Release	OSPS-BR-05	All build and release pipelines MUST use standardized tooling where available to ingest dependencies at build time.	Ensure that th release pipeli tools and proc dependencies compatibility i vulnerabilities									1.2b, 1.2d, 1.2f, 1.2h, 1.2j, 2.1, 2.2, 2.3	PO3.2, PS1, PS2			483-813, 124-564, 347-352,715-334
Build & Release	OSPS-BR-05.01															
Build & Release	OSPS-BR-06	Produce all released software assets with signatures and hashes.	All released s be signed or a signed manife asset's crypto										PO5.2, PS2, PS2.1, PW6.2			
Build & Release	OSPS-BR-06.01															
Documentation	OSPS-DO-01	The **project documentation** MUST provide user guides for all basic functionality.	Ensure that us comprehensiv project's curre prevent dama									1.2b, 1.2j, 1.2k	PW1.2	GV.OC-04, GV.OC-05	4.1.4	036-275

OSPS-BR-04 - All releases MUST provide a descriptive log of functional and security modifications.

Provide transparency and accountability for changes made to the project's software releases, enabling users to understand the modifications and improvements included in each release.

OSPS-BR-04.01

Requirement: When an official release is created, that release MUST contain a descriptive log of functional and security modifications.

Recommendation: Ensure that all releases include a descriptive change log. It is recommended to ensure that the change log is human-readable and includes details beyond commit messages, such as descriptions of the security impact or relevance to different use cases. To ensure machine readability, place the content under a markdown header such as "## Changelog".

- Maturity Level 2
- Maturity Level 3

External Framework Mappings

- **BPB**: CC-B-8, CC-B-9
- **CRA**: 1.2l, 2.2
- **SSDF**: PS1, PS2, PS3, PW1.2
- **OCRE**: 486-813, 124-564, 745-356

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

https://docs.google.com/spreadsheets/d/1an5mx3rayoz3JRFUepD56zgprpwXBXBG70fVZvIMCpA/

Building a Better Catalog

Baseline currently maps alignment across multiple cyber compliance frameworks and/or cyber legislations. “Baselining” helps downstream select projects that align with and that support their compliance obligations!

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- SSDF
- CSF
- 800-161/800-53
- CISA Software Acquisition Guide (forthcoming)

European Commission

- Cyber Resilience Act
- DORA (forthcoming)

National Cyber Security Centre
a part of GCHQ

- Software Security Code of Practice (forthcoming)

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

- BP Badges
- Scorecard
- Minder
- SLSA
- OpenSSF tooling

PCI Security Standards Council

SAMM

OPENCRE

OPENCHAIN

Proactive Software Supply Chain Risk Management (P-SSCRM) Framework

Have a framework or a particular piece of legislation you’d like to see integrated into the Baseline? [Patches Welcome]!

Why Baseline Matters

Value-prop for Devs

- Gives **direct** and **actionable** advice for improving security practices
- Provides the ability for Developers/projects to show they follow reasonable security measures as well as ways to improve
- **Allow projects to humble-brag** about how great they are
- **Collects common downstream requests** (nags/demands) and advertises them **so Downstream can RTFM** and stop harassing their unpaid Upstream component sources

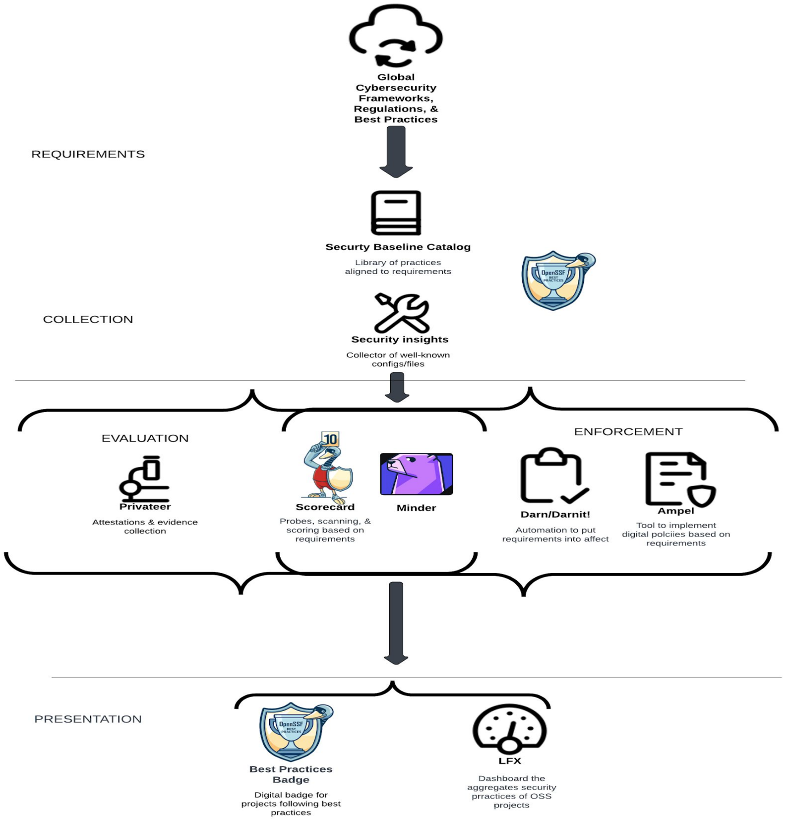
Value-prop for Downstream

- Provides **clear signals** and **evidence/attestations** about upstream component security practices *to allow corporate due-diligence and risk management*
- Provides a **clear checklist** of things that Downstream could go work with (donate/DO) for their Upstream sources
- **Aligns software development practices with global cybersec laws** and frameworks (reduces compliance costs [do once, applicable many])

Future Workflow

- Baseline Catalog v1.0 is ready today!
- Compliance Crosswalk 1.0 ready today!
- Tooling to enable and empower the Baseline Catalog are being developed TODAY!

Follow the ORBIT Working group (Open Resources for Baselines, Interoperability, and Tooling) for more details - https://github.com/ossf/wg-orbit



Global Cybersecurity Frameworks, Regulations, & Best Practices

REQUIREMENTS

Securty Baseline Catalog

Library of practices aligned to requirements

COLLECTION

Security insights

Collector of well-known configs/files

EVALUATION

Privateer

Attestations & evidence collection

Scorecard

Probes, scanning, & scoring based on requirements

Minder

ENFORCEMENT

Darn/Darnit!

Automation to put requirements into affect

Ampel

Tool to implement digital polciies based on requirements

PRESENTATION

Best Practices Badge

Digital badge for projects following best practices

LFX

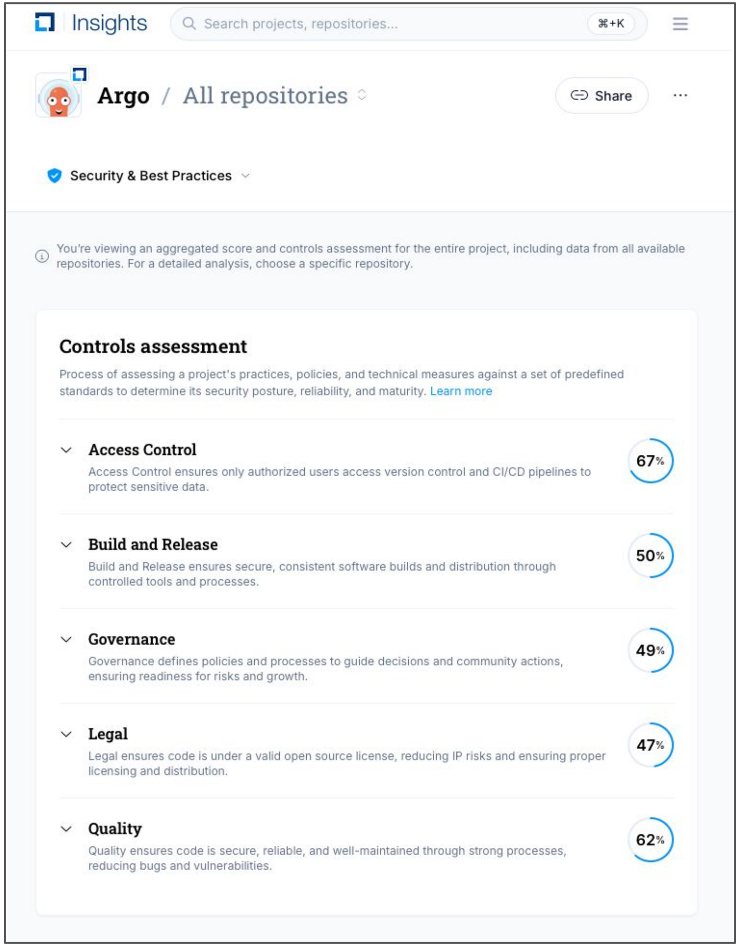
Dashboard the aggregates security prractices of OSS projects

Tying it all together

As the group settles into a working rhythm, we’re now ready to start engaging with the broader LF and ecosystem.

We’ll begin work on a “Baseline workflow” on how projects can “Get Baselined”, work on docs, education, and continue work on automation and attestations .

Tools Like LFX, Scorecard, and BP Badges will be outward signs for developers and consumers about the “Baselineness” of a project.



You're viewing an aggregated score and controls assessment for the entire project, including data from all available repositories. For a detailed analysis, choose a specific repository.

Controls assessment

Process of assessing a project's practices, policies, and technical measures against a set of predefined standards to determine its security posture, reliability, and maturity. Learn more

Access Control 67%
Access Control ensures only authorized users access version control and CI/CD pipelines to protect sensitive data.

Build and Release 50%
Build and Release ensures secure, consistent software builds and distribution through controlled tools and processes.

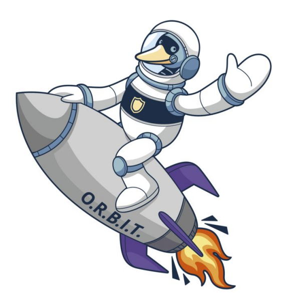
Governance 49%
Governance defines policies and processes to guide decisions and community actions, ensuring readiness for risks and growth.

Legal 47%
Legal ensures code is under a valid open source license, reducing IP risks and ensuring proper licensing and distribution.

Quality 62%
Quality ensures code is secure, reliable, and well-maintained through strong processes, reducing bugs and vulnerabilities.

How to get involved…

- Review the Baseline, give feedback
- Consider implementing the Baseline criteria for projects you work on
- As a Consumer, consider using Baseline as part of your third-party component due-diligence
- Suggest additional cyber frameworks or legislation to add to the Compliance Crosswalk
- Participate in the new “Baseline for AI” project
- Attend a Baseline or ORBIT meeting to contribute to the Catalog and Tooling



Baseline

ORBIT

10

Ways to Participate

- Join a Working Group/Project
- Come to a Meeting (see Public Calendar)
- Collaborate on Slack
- Contribute on GitHub
- Become an Organizational Member
- Keep up to date by subscribing to the OpenSSF Mailing List

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Thank You

Legal Notice