OpenSSF
OPEN SOURCE SECURITY FOUNDATION

How many security badges do we need?



Arnaud Le Hors lehors@us.ibm.com
5 Nov 2026

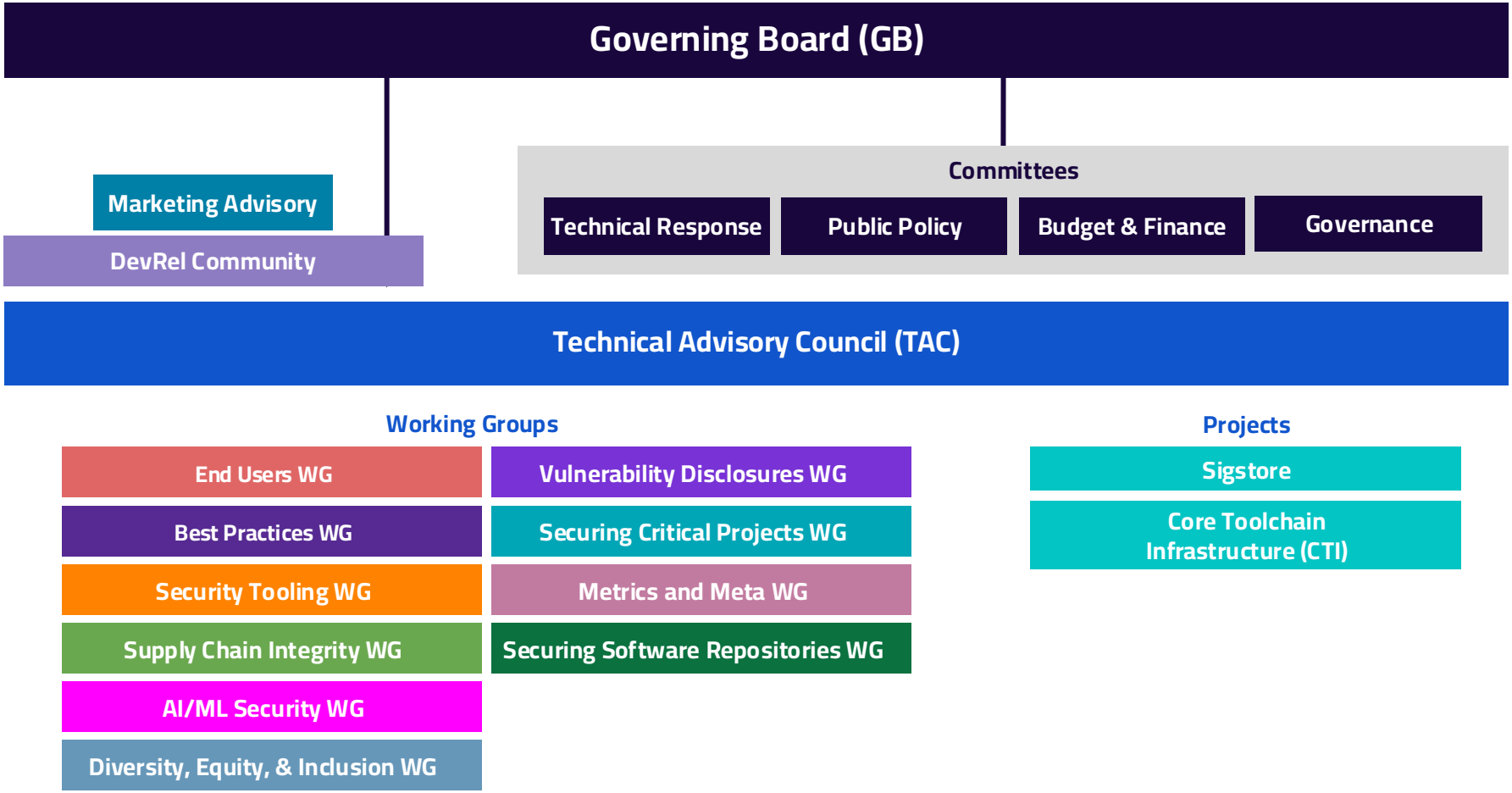
OSS, Security, & OpenSSF



- Millions of OSS projects
- Many foundations run OSS projects relevant to security and/or DevSecOps
  - LF Foundations: Continuous Delivery Foundation, Cloud Native Computing Foundation, etc.
  - Other foundations: Apache Software Foundation, Eclipse Foundation, Python Software Foundation, OWASP, etc.

- Open Source Security Foundation (OpenSSF)
  - “Collaboration and working both upstream and with existing communities to advance open source security for all”
  - Formed in Aug 2020, relaunched properly in Sep 2023

OpenSSF Structure



OpenSSF Working Groups



AI/ML Security



BEAR

Belonging, Empowerment, Allyship, and Representation



BEST

Best Practices for Open Source Developers



Global Cyber Policy



ORBIT

Open Resources for Baselines, Interoperability, and Tooling



Securing Critical Projects



Securing Software Repositories



Security Tooling



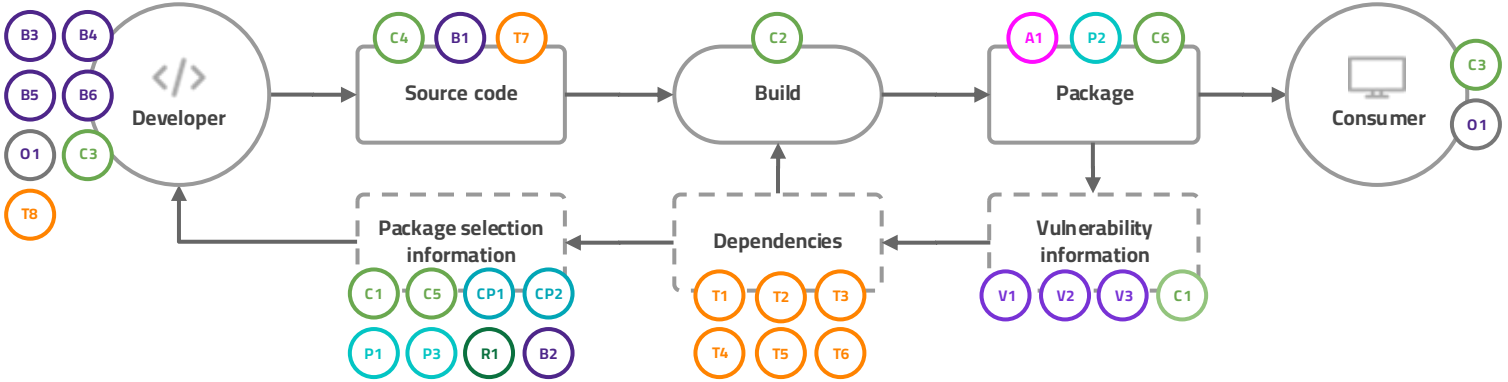
Supply Chain Integrity



Vulnerability Disclosures

Visit the Working Groups page at https://openssf.org/community/openssf-working-groups/ for information on each group.

OpenSSF Technical Initiatives Landscape



Best Practices
B1. OpenSSF Best Practices Badge project
B2. OpenSSF Scorecard project
B3. Education SIG
B4. Memory Safety SIG
B5. C/C++ Compiler Options SIG
B6. Python Hardening SIG

Global Cyber Policy

DevRel Community

AI/ML Security
A1. Model Signing SIG & Project

Supply Chain Integrity
C1. Security Insights project
C2. SLSA project
C3. S2C2F project
C4. Gittuf project
C5. GUAC project
C6. Zarf project M

BEAR (Belonging, Empowerment, Allyship, and Representation)

Securing Software Repositories
R1. RSTUF Project

Security Tooling
T1. SBOM Everywhere SIG
T2. OSS Fuzzing SIG
T3. SBOMit project
T4. Protobom project
T5. bomctl project
T6. Fuzz Introspector project
T7. Minder project
T8. OpenBao project

Vulnerability Disclosures
V1. CVD Guides SIGs
V2. OSV Schema project
V3. OpenVEX SIG
OpenVEX Project

Securing Critical Projects
CP1. criticality_score project
CP2. Package Analysis project

ORBIT (Open Resources for Baselines, Interoperability, and Tooling)
O1. OSPS Baseline project

Projects
P1. Alpha & Omega project
P2. Sigstore
P3. Core Toolchain Infrastructure (CTI)

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF Scorecard

Quickly assess open source projects for risky practices.



OpenSSF Scorecard: Use Cases

For individual maintainers

- Helpful as a pre-launch security checker for a new project or to plan improvements to an existing one.

For an organisation

- Include in CI/CD processes using the GitHub action and run by default on pull requests.

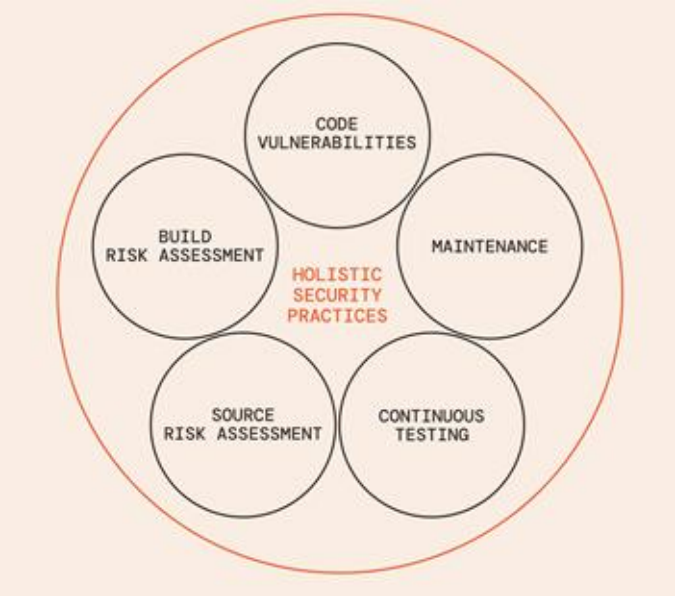
For consumers

- Helps to make informed decisions about security risks and vulnerabilities.
- Using the public data, evaluate the security posture of over 1 million of the most used OSS projects.

Automated Checks with Weighted Scoring

- 18 checks for vulnerabilities affecting different parts of the software supply chain (shown right)
- Each automated check returns a score out of 10 and a risk level; some checks have staged scoring, others are dichotomous
- The risk level adds weighting to the score (shown below)
- The weighted value of all checks are compiled into a single, aggregate score

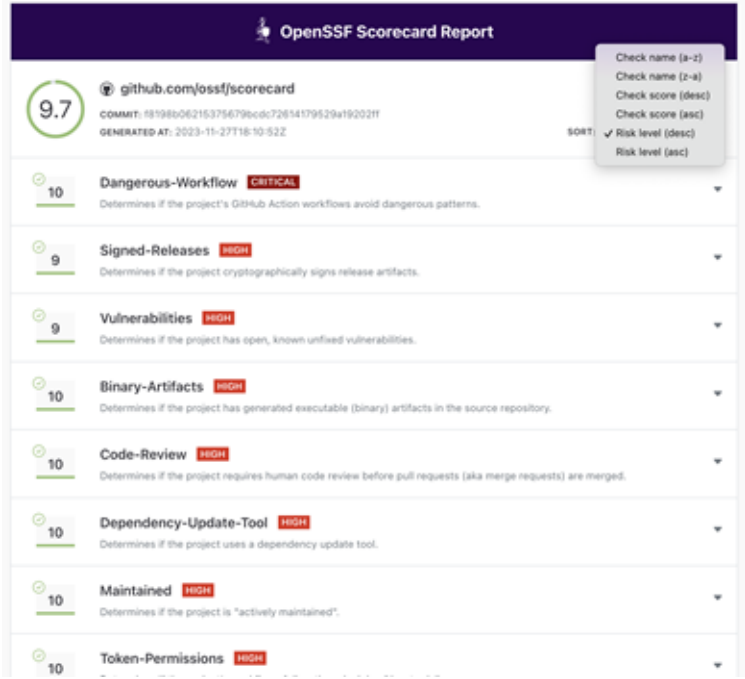
CRITICAL RISK	10
HIGH RISK	7.5
MEDIUM RISK	5
LOW RISK	2.5



https://github.com/ossf/scorecard#scorecard-checks

OpenSSF Scorecard: Viewing Scores

- Use the webviewer to see score reports for projects regularly scanned by Scorecard (shown right, link below)
  - https://securityscorecards.dev/viewer/?uri=<github_or_gitlab>.com/ <user_name_or_org>/<repository_name>
  - Results can be sorted by check name, score, or risk level
- Use the REST API to query pre-calculated scores of OSS projects
- Use the Scorecard CLI to view scores for projects that are not regularly scanned by Scorecard
- OpenSSF Scorecard scans ***1 million*** of the most critical OSS projects
  - Results published in a BigQuery public dataset



OpenSSF Scorecard: Showing your badge

- To add a badge to your README, copy and paste the below line, and replace the {owner} and {repo} parts:

[![openssf_scorecard](https://api.scorecard.dev/projects/github.com/{owner}/{repo}/badge)](https://scorecard.dev/viewer/?uri=github.com/{owner}/{repo})

- Once this badge is added, clicking on the badge will take users to the latest run result of Scorecard.



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Best Practices Badge Program

Best practices for Free/Libre and Open Source Software



Best Practices Badge Program

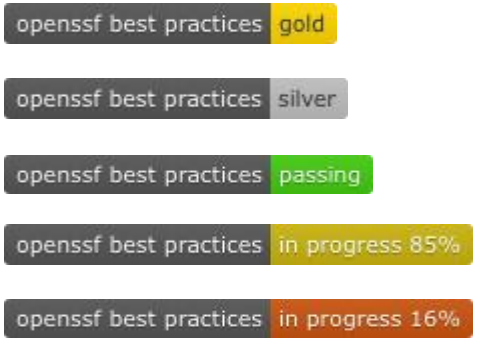
The OpenSSF Best Practices Badge website outlines the criteria for the passing badge, provides an example, shows participating projects, and supports queries to show projects that have a passing badge. This project was formerly known as the Core Infrastructure Initiative (CII) Best Practices Badge and was formally renamed as part of OpenSSF in late 2021. More information on the OpenSSF Best Practices Badging program is available on GitHub.



Best Practices Badge Program

Getting a passing badge is a significant achievement; on average only about 10% of pursuing projects have a passing badge. We have established two higher levels beyond passing: silver and gold. Here is a summary of the gold criteria:

- At least 2 unassociated significant contributors
- Per-file copyright and license
- Use 2FA
- At least 50% of all modifications are reviewed by another
- Have a reproducible build
- Use continuous integration
- Statement coverage 90%+
- Branch coverage 80%+
- Support secure protocols & disable insecure protocols by default
- Use TLS version 1.2 or higher
- Have a hardened project website, repo, and download site
- Have a security review (internal or external)



OSPS Baseline

Structured security requirements aligned with international frameworks, standards, and regulations



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.

All your Base are belong to us





The OpenSSF Security Baseline was officially released Feb 2025

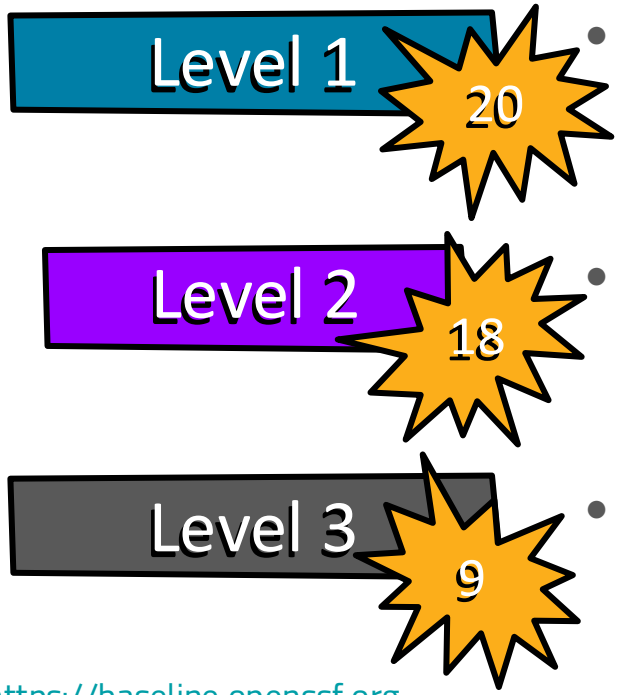
Based on a library of well-known cybersecurity frameworks, standards, and global regulations

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.

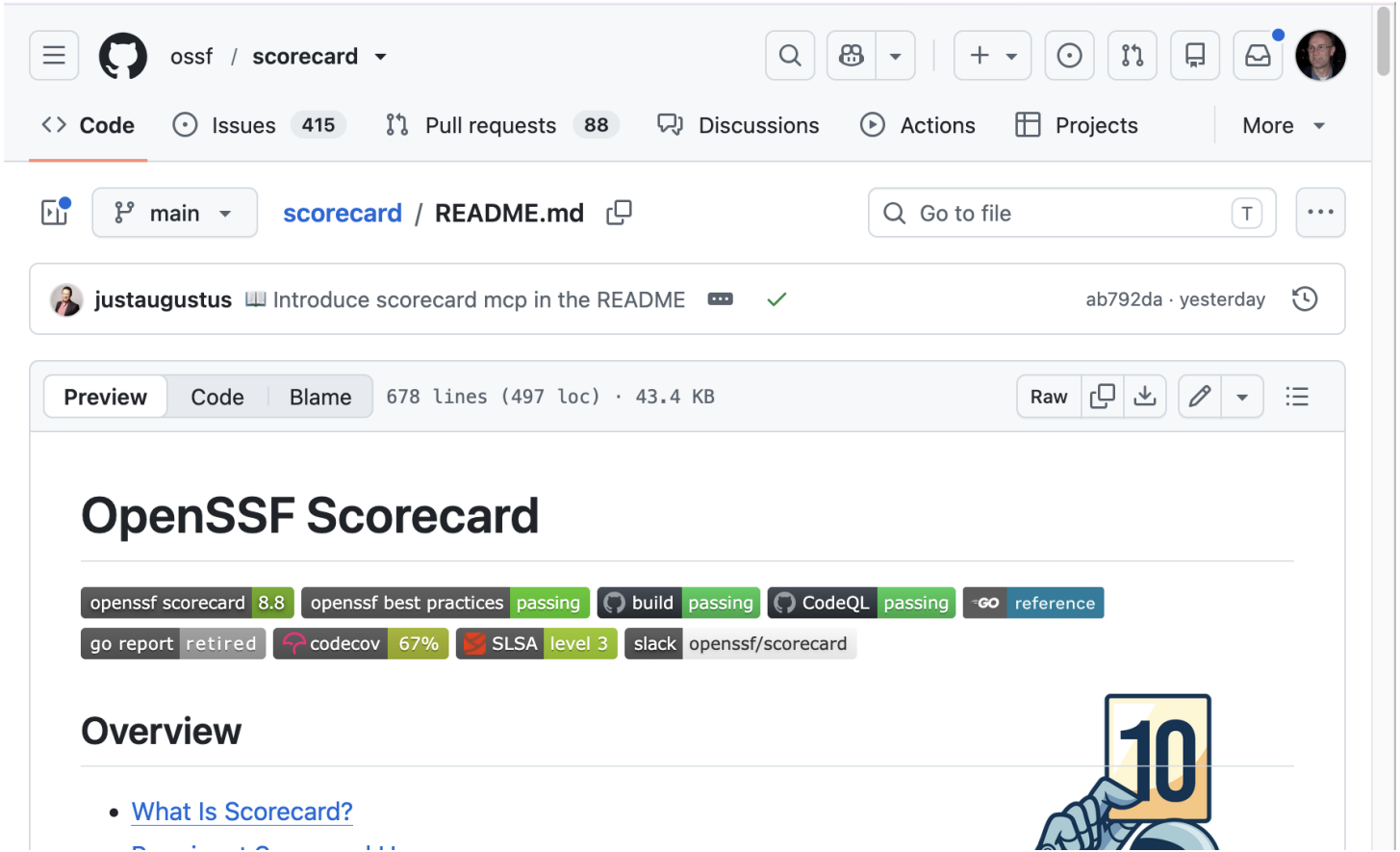
https://baseline.openssf.org
https://github.com/ossf/security-baseline



The challenge

Which badges to aim for?

How many badges can one get?



Maintainer experience

Feedback from “webchick” to OpenSSF TAC on May 29, 2023 :

However, by and large, open source maintainers:

- Have very little time for "extracurricular activities" beyond their maintainer responsibilities, since they are often balancing these with a job and a family
- Therefore, tend to "silo" into their own projects, their own community, and their own problems, by necessity
- *Therefore*, be broadly unaware of OpenSSF's existence — if they go to events, and have $1000 to spend on a ticket, they will tend to attend something like DrupalCon, not something like Open Source Summit
- Once learning of OpenSSF's existence, they will have very little time to dig through information (including terms/acronyms they may not already be familiar with, such as "SBOMs") to answer the question "What are the problems you solve for my project and how do I partner with you?"
- When they attempt to answer this question based on the available information, they'll see a lot of evidence of how OpenSSF helps enterprises, governments, etc. and *their* customers, but not a lot of information of how it helps them as an everyday maintainer. (They may in fact leave with the *opposite* impression, that the OpenSSF exists to make their job *harder*, in order to please enterprises / customers :\ — see the blow-up when YubiKeys were distributed to maintainers of all the top Python projects, for example.)

https://github.com/ossf/tac/issues/169

Thoughts

- Having too many security badges/programs is counter productive, the number is overwhelming maintainers and organizations.
- Yet, more are coming all the time.
- Tip: getting anyone of them is better than none though! ☺
- Open question: Can anything be done to bring convergence ?

This presentation released under the CC-BY-4.0 license

This overall presentation is released under the Creative Commons Attribution 4.0 International (CC-BY-4.0). You are free to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material

for any purpose, even commercially. This license is acceptable for Free Cultural Works. The licensor cannot revoke these freedoms as long as you follow the license terms. Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits

For full details, see: creativecommons.org/licenses/by/4.0/