SmartSuite

Framework / Software Security / OWASP

OWASP Software Assurance Maturity Model (SAMM) version 2.0

OWASP SAMM 2.0 is the OWASP Foundation's open maturity model for software security: 15 practices in five business functions, each scored on three maturity levels, with a roadmap to improve.



What it is

OWASP SAMM, the Software Assurance Maturity Model, is the OWASP Foundation's open framework for analyzing and improving an organization's software security posture; version 2.0 has been the current model since its release in early 2020 (GitHub release v2.0 on February 3, 2020) and is maintained incrementally on owaspsamm.org rather than as a single document. Adoption is voluntary: any organization that develops, buys or operates software can use it, and SAMM's stated mission is to give all types of organizations an effective and measurable way to analyze and improve their software security posture.

The model is built around 15 security practices grouped into five business functions: Governance, Design, Implementation, Verification and Operations. Each business function has three security practices; each practice contains activities arranged in logical flows and divided into two streams with their own objectives; and each practice is scored on three maturity levels, where level 1 is initial implementation, level 2 structured realization and level 3 optimized operation. SAMM is prescriptive and fully defined, technology and process agnostic, and supports waterfall, iterative, agile and DevOps development.

At a glance

PUBLISHER Open Worldwide Application Security Project (OWASP)	TYPE Assessment / Maturity Model	VERSION 2.0 (February 2020), maintained incrementally on owaspsamm.org
EFFECTIVE February 3, 2020	DOMAIN Software Security	FAMILY OWASP
REGION International	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: owaspsamm.org/

Why it matters

- **A shared map of software security work** Five business functions and 15 security practices give every team the same vocabulary, from Strategy and Metrics in Governance to Operational Management in Operations.
- **A score that can be repeated** Three maturity levels per practice, with quality criteria for every activity and an updated scoring model in version 2.0, let an organization measure coverage and quality and compare one assessment with the next.
- **Targets the organization chooses** Each organization determines the target maturity level for each security practice that is the best fit for it, rather than meeting a fixed bar.
- **Works with any development style** The version 2 model is development paradigm agnostic and supports waterfall, iterative, agile and DevOps, so the same assessment applies across teams that build differently.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports OWASP SAMM

Practice Maturity Assessment

Record each of the 15 security practices with its current score on the three maturity levels, by stream, using the version 2.0 coverage and quality criteria as the scoring fields.

Target Maturity per Practice

Capture the target level the organization chooses for each practice, as the model prescribes, together with the gap between current and target.

Improvement Roadmap

Turn gaps into a phased roadmap with owners, milestones and due dates, following the defined iterations the Getting Started guide describes.

Activity Evidence Library

Attach the evidence behind each activity in Compliance Management, from Governance policies to Operations incident records, so the next assessment starts from a record.

Assessment Round Reporting

Use dashboards to show maturity by business function and practice and the change from one assessment round to the next.

Version 1.5 to 2.0 Mapping

Keep OWASP's published mapping from version 1.5 to 2.0 beside each practice record so teams with an older assessment can carry it over.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | MITRE ATT&CK | NIST 800-218 SSDF | OWASP ASVS 4.0 | OWASP Top 10 2021

Official resources

OWASP SAMM project site

The SAMM v2 project site, with the model, documentation, assessment toolbox and benchmark.

owaspsamm.org

OWASP SAMM Model

The five business functions, fifteen security practices and three maturity levels that make up SAMM v2.

owaspsamm.org/model

OWASP SAMM Assessment Toolbox

The assessment toolbox for scoring an organization's maturity against each SAMM practice and planning improvement.

owaspsamm.org/assessment

OWASP SAMM Benchmark

The benchmark initiative that lets organizations compare their SAMM scores with peers.

owaspsamm.org/benchmark

Frequently asked questions

What are the five business functions and 15 security practices in OWASP SAMM 2.0?

Governance (Strategy and Metrics; Policy and Compliance; Education and Guidance), Design (Threat Assessment; Security Requirements; Secure Architecture), Implementation (Secure Build; Secure Deployment; Defect Management), Verification (Architecture Assessment; Requirements-driven Testing; Security Testing) and Operations (Incident Management; Environment Management; Operational Management). Each business function is a category of activities that any organization involved with software development must fulfill to some degree, and each has exactly three security practices.

How do the three SAMM maturity levels work?

Every security practice is scored on three maturity levels: level 1 is initial implementation, level 2 structured realization and level 3 optimized operation. Each level has a successively more sophisticated objective, specific activities and stricter success metrics, and activities at a lower level are typically easier to execute and need less formalization. The activities of a practice are divided into two streams, each with an objective reached in increasing levels of maturity, and version 2.0 scores maturity for both coverage and quality using quality criteria defined for every activity.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What is the current version of OWASP SAMM and when was it released?

Version 2.0 is the current model; the model page on owaspsamm.org is labeled SAMM Version 2.0 and the GitHub release v2.0 is dated February 3, 2020, after three years of preparation. Since version 2.0 the main publication channel is the OWASP SAMM website rather than a monolithic document, with content in YAML files and small incremental updates, so there is no later numbered edition. The model is licensed under Creative Commons Attribution-ShareAlike 4.0.

What changed from SAMM 1.5 to SAMM 2.0?

The release notes list the major changes: a fifth business function, Implementation, with the new Defect Management practice; Construction renamed Design; a redesigned Verification function; Operational Management added and Operational Enablement removed; activities presented in logical flows across the 15 practices and divided into two streams with their own objectives; maturity measured by coverage and quality with new quality criteria and an updated scoring model; and a single GitHub source that generates the PDF, website and toolbox. OWASP publishes a mapping from version 1.5 to 2.0.

Does an organization have to reach maturity level 3 in every practice, and is SAMM a certification?

No on both counts. SAMM does not insist that all organizations achieve the maximum maturity level in every category; each organization determines the target maturity level for each security practice that is the best fit and adapts the templates to its own needs. SAMM is a self-assessment model supported by the SAMM Toolbox for assessments and roadmaps and the SAMM Benchmark for comparing results with similar organizations, not a certification scheme.

License included / downloadable: Yes OWASP SAMM is free of charge on owaspsamm.org under the Creative Commons Attribution-ShareAlike 4.0 license, with the model content published as open YAML files.

Full framework page and mappings: smartsuite.com/frameworks/owasp-samm-software-assurance-maturity-model

© 2026 SmartSuite Inc. All rights reserved.