

OWASP SAMM 2.0

OWASP SAMM is a framework for assessing and improving an organization's software security practices and maturity across the SDLC.



What it is

OWASP SAMM (Software Assurance Maturity Model) is an open-source cybersecurity and software assurance framework that helps organizations evaluate, develop, and improve their secure software development practices. The model provides a structured approach to measuring and enhancing the maturity of processes related to software security throughout the software development lifecycle (SDLC).

Published by the Open Web Application Security Project (OWASP), SAMM is used by development teams, security professionals, and compliance leaders to assess and strengthen areas such as governance, design, implementation, verification, and operations. It supports a range of organizations, from startups to large enterprises, seeking to manage software-related security risks and align with regulatory or industry requirements.

At a glance

PUBLISHER Open Web Application Security Project (OWASP)	TYPE Assessment / Maturity Model	VERSION OWASP SAMM v2
EFFECTIVE 2012	DOMAIN Software Security	FAMILY OWASP
REGION United States	ADOPTION MODEL Operational Security	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://owasp.org/www-project-samm/>

Why it matters

- **Strengthen software security governance** Foster clear policies and accountability, enabling leadership to oversee and guide secure development practices across projects.
- **Enhance regulatory compliance support** Align software assurance processes with industry and legal requirements, helping meet obligations and reducing risk of non-compliance.
- **Promote continuous process improvement** Establish structured maturity assessments and roadmaps to systematically identify gaps and drive ongoing security enhancement.
- **Improve incident detection and response** Enable organizations to recognize and address software-related vulnerabilities more rapidly throughout the software lifecycle.

How SmartSuite supports OWASP SAMM

Maturity Assessments by Practice

Run SAMM assessments with scoring and evidence for each practice area.

Improvement Roadmap and Ownership

Turn gaps into a prioritized roadmap with owners, milestones, and due dates.

Evidence for Secure SDLC Practices

Centralize proof for governance, design, implementation, verification, and operations.

Metrics and Program Reporting

Track maturity trends and KPIs to show measurable improvement.

Cross-Team Standardization

Standardize practices and templates across product teams for consistency.

Executive Reporting Dashboards

Report maturity, gaps, and progress at the program and product level.

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 v2.0 Official Guide

Provides a comprehensive overview and detailed guidance on implementing OWASP SAMM.

owaspsamm.org

OWASP SAMM Assessment Model

Outlines tools and methodologies for assessing software assurance maturity using SAMM.

owaspsamm.org/model

OWASP SAMM Design & Implementation Guidance

Details practical advice for adopting OWASP SAMM in software development processes.

owaspsamm.org/model/design

OWASP SAMM Operational Support Resources

Describes resources available for ongoing support and enhancement of SAMM implementations.

owaspsamm.org/model

Frequently asked questions

What is OWASP SAMM used for?

OWASP SAMM is used to assess, improve, and manage secure software development practices across the software development lifecycle (SDLC). It provides organizations with a structured maturity model to measure, benchmark, and enhance software security processes within development teams and the broader organization.

Is OWASP SAMM certifiable or mandatory?

OWASP SAMM is not a certifiable or mandatory framework. It is a self-assessment model designed to guide organizations in maturing their software assurance practices and aligning with regulatory or industry best practices rather than providing formal certification.

Who should use OWASP SAMM, and what is its scope?

OWASP SAMM is applicable to organizations of any size that develop, deploy, or manage software applications. It is commonly used by security professionals, development teams, and compliance leaders to evaluate and improve software security throughout governance, design, implementation, verification, and operations functions.

What are the key concepts and artifacts in OWASP SAMM?

Key concepts in OWASP SAMM include business functions, security practices, maturity levels, and related activities. Artifacts such as maturity assessment results, gap analyses, improvement roadmaps, and evidence of implemented controls are central to tracking progress and supporting compliance initiatives.

How does an organization implement OWASP SAMM in practice?

Organizations implement OWASP SAMM by conducting a baseline maturity assessment, identifying gaps in current software security controls, and prioritizing areas for improvement. Implementation typically involves aligning SAMM practices with internal governance structures and integrating improvements into existing development workflows.

How does OWASP SAMM relate to other security and compliance frameworks?

OWASP SAMM complements established frameworks like ISO 27001, NIST, and PCI DSS by providing a focused approach to software security maturity. It can be integrated into broader security, risk, and compliance programs to enhance application security controls and meet overlapping regulatory requirements.

What are the ongoing compliance requirements when using OWASP SAMM?

Ongoing compliance with OWASP SAMM involves regular reassessment of software security maturity, continuous monitoring of implemented controls, and iterative improvements based on assessed risks. Documentation, evidence collection, and reporting support audit readiness and ensure that security improvements are sustained over time.

How would SmartSuite support OWASP SAMM?

SmartSuite supports OWASP SAMM by offering pre-built control libraries mapped to SAMM practices, risk tracking, and automated evidence collection. The platform enables organizations to manage assessments, remediation activities, and compliance documentation while maintaining audit readiness and providing comprehensive reporting on software assurance maturity.

License included / downloadable: Yes OWASP SAMM is published by the OWASP Foundation and is publicly available as an open security framework.

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