



OWASP SAMM Update

SAMM User Day

June 16th, 2020

Bart De Win, Seba Deleersnyder

What is SAMM?

OWASP
FLAGSHIP
mature projects

The mission of OWASP SAMM is to be the prime maturity model for software assurance that provides an effective and measurable way for all types of organizations to analyze and improve their software security posture. OWASP SAMM supports the complete software lifecycle, including development and acquisition, and is technology and process agnostic. It is intentionally built to be evolutive and risk-driven in nature.



Visit our website

owaspsamm.org

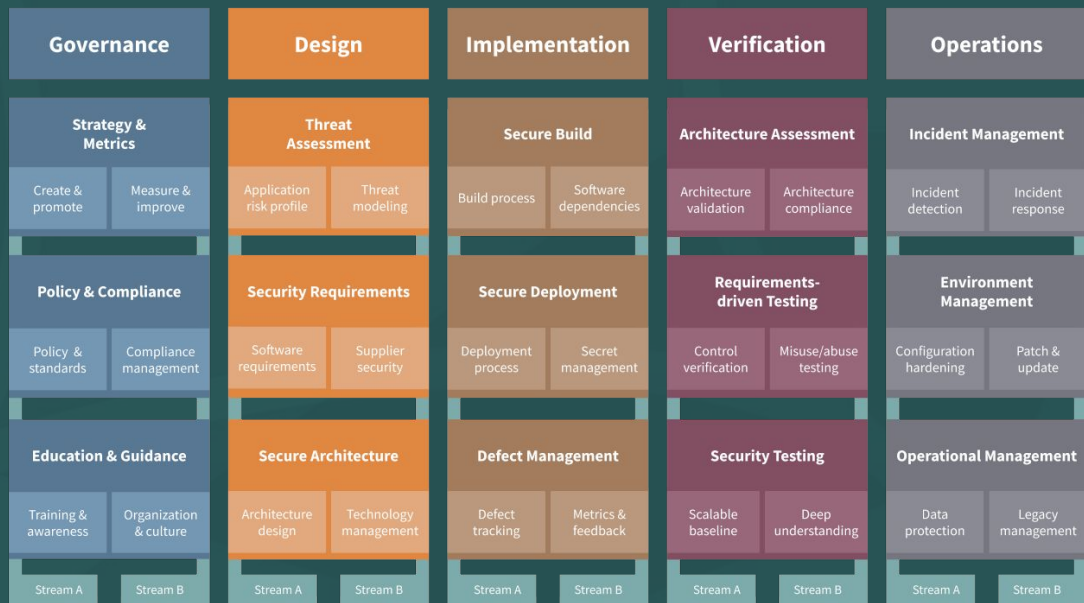


Goals of SAMM version 2

- Align with recent development practices
- Revise all activities (no “orphans”)
- Method agnostic
- Improve assessments
- Improve production process

Backwards compatibility was not a goal

Core structure





SAMM v2

security practice structure

	A: Control Verification	B: Misuse /Abuse Testing
Level 1 - <i>Opportunistically find basic vulnerabilities and other security issues.</i>	Test for standard security controls	Perform security fuzzing testing
Level 2 - <i>Perform implementation review to discover application-specific risks against the security requirements.</i>	Derive test cases from known security requirements	Create and test abuse cases and business logic flaw test
Level 3 - <i>Maintain the application security level after bug fixes, changes or during maintenance</i>	Perform regression testing (with security unit tests)	Denial of service and security stress testing

SAMM v2

security practice structure

Level 1 - *Opportunistically find basic vulnerabilities and other security issues.*

Level 2 - Perform **implementation review** to discover **application-specific risks** against the security requirements.

Level 3 - **Maintain** the application security level after bug fixes, changes or during maintenance

MATURITY

SAMM v2

security practice structure

STREAMS

A: Control Verification

**B: Misuse /Abuse
Testing**

Test for standard security controls

Perform security fuzzing testing

Derive test cases from known security requirements

Create and execute abuse cases and business process flaw test

Perform regression testing (with security unit tests)

Denial of service and security stress testing

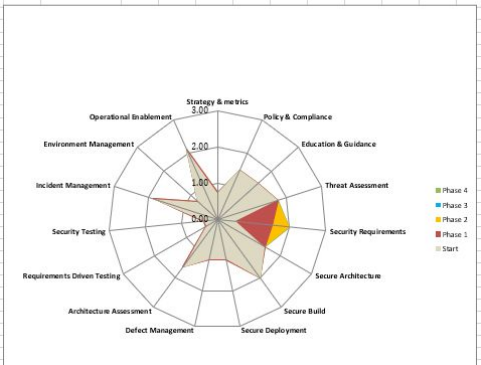
SAMM v2 assessment toolbox

GOVERNANCE

Stream	Level	Strategy and metrics
Create and promote	1	Has the organization defined a set of risks to prioritize applications by?
		<ul style="list-style-type: none">• You have captured the risk appetite of your organization's executive leadership• The organization's leadership have vetted and approved risks• You have identified the main business and technical threats to your organization's assets and data• Risks are documented and accessible to relevant stakeholders

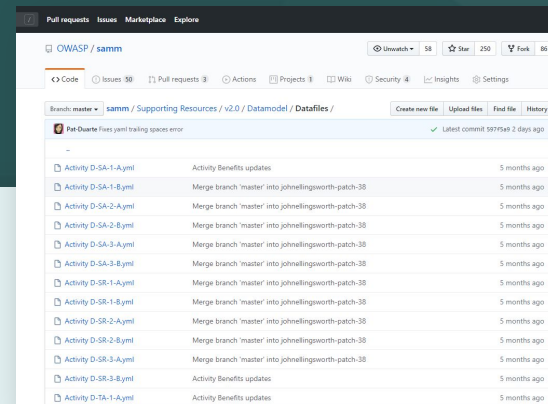
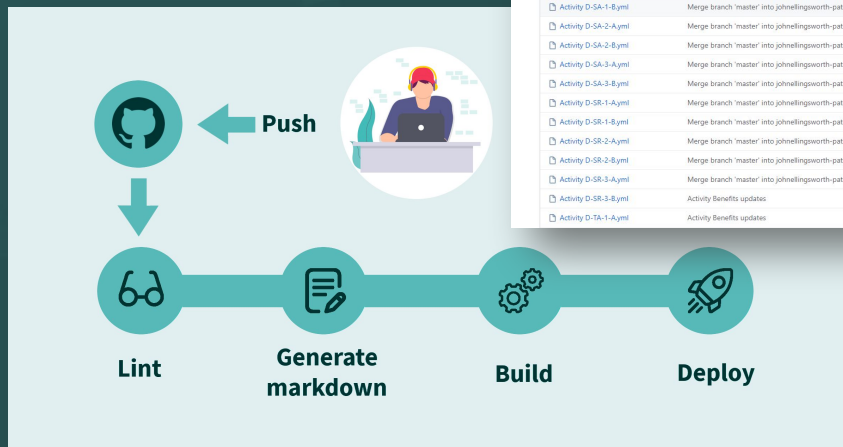
<https://github.com/OWASP/samm/tree/master/Supporting%20Resources/v2.0/toolbox>

SAMM roadmaps

[illegible]

Project: SAMM CI/CD

- Single source of the truth (Github)
- Used to generate everything *automatically*
 - Document, website
 - Toolbox
 - Applications



Community involvement

Project
driven

Core structure

Business functions, practices, streams

Evaluation model

Questions, quality criteria, measurement model

Activity model

Objective, activities, dependencies, metrics

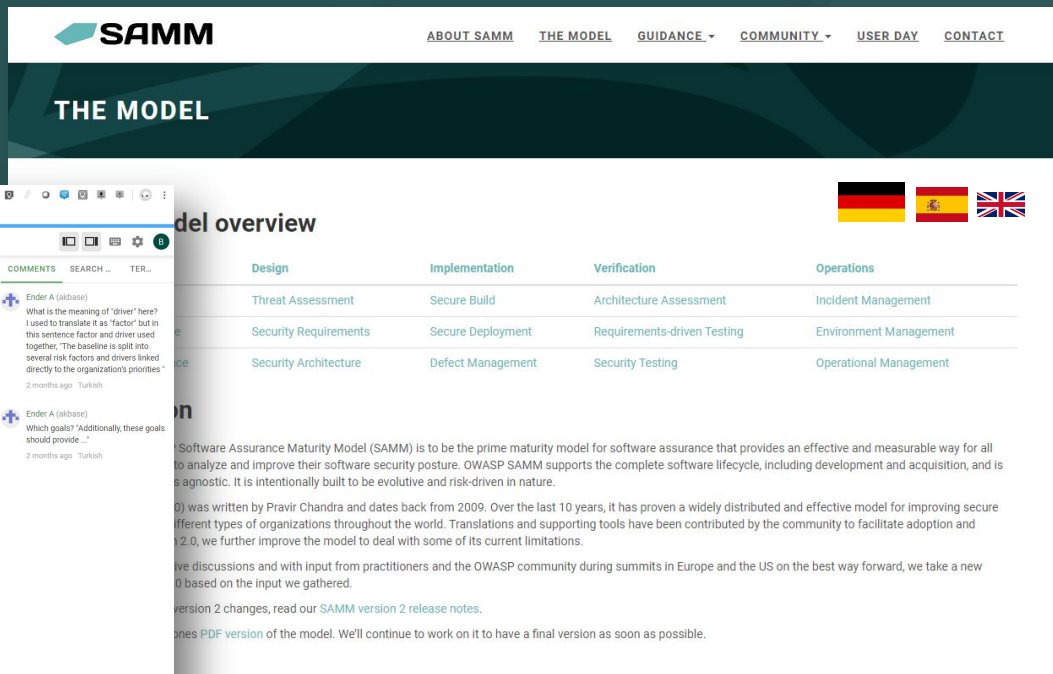
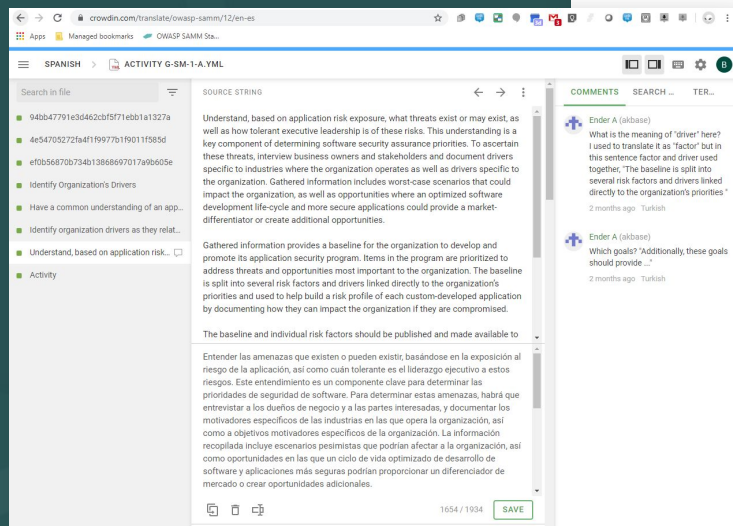
Community
driven

Supporting information & tools

Guidance, references, supporting tools


Community
feedback

Translations



<https://crowdin.com/project/owasp-samm>

How do I compare?

 [ABOUT SAMM](#) [THE MODEL](#) [GUIDANCE ▾](#) [COMMUNITY ▾](#) [USER DAY](#) [CONTACT](#)

BENCHMARKING

SAMM Benchmarking

Goals

OWASP SAMM (Software Assurance Maturity Model) Benchmarking is a sub-project within OWASP SAMM to facilitate information and data collaboration between organizations with the goal to help answer the critical questions "How am I doing?" and "What might be working for other similar organizations".

The goal of this project is to collect the most comprehensive dataset related to organizational maturity of application or software security programs. Allowing OWASP SAMM to enable comparative analysis for the SAMM practioners and other future research as well. This data should come from both self-assessing organizations and consultancies that perform third party assessments.

We will accept data from SAMM v1.5 and SAMM v2.x and beyond. There will be support for partial comparisons between SAMM v1.5 and SAMM v2.x, but as the model will undergo breaking changes for v2.0 it will not be a full comparison between the versions. We plan to support multiple submissions from the same organization over time so that progress can be shown on the dashboard.

Analysis Infrastructure

The plan is to leverage the OWASP Azure Cloud Infrastructure to collect, analyze, and store the data contributed. There will be a minimal number of administrators that have access to manage the raw data. Dashboards and comparative analysis will be performed with data that is aggregated and/or separated from the submitting organization (additional details in the Process section).

Contributions

We plan to support both known and pseudo-anonymous contributions. The preference is for contributions to be known; this immensely helps with the validation/quality/confidence of the data submitted. If the submitter prefers to have their data stored anonymously and even go as far as submitting the data anonymously, then it will have to be classified as "unverified" vs. "verified".

Our roadmap

- Continuous: minor fixes
- Wrap-up: PDF
- v2.1 (Oct 2020): Translations, mappings
- v2.2 (Jan 2021): Activity-specific guidance (references, agile, ...)
- V2.3 (June 2021): online toolbox, open API
- V3.0: tbd

Let's do this together



Who is SAMM?

Bart De Win Project Co-Leader, Belgium	Sebastien (Seba) Deleersnyder Project Co-Leader, Belgium
Brian Glass – United States	Daniel Kefer – Germany
Yan Kravchenko – United States	Chris Cooper – United Kingdom
John DiLeo – New Zealand	Nessim Kisserli – Belgium
Patricia Duarte – Uruguay	John Kennedy – Sweden
Hardik Parekh – United States	John Ellingsworth – United States
Sebastián Arriada – Argentina	Brett Crawley – United Kingdom

SAMM Sponsors



owaspsamm.org/sponsors

Enjoy the User Day !



Time (UTC)	Type	Title	Speaker
12.00	Talk	OWASP SAMM Update	Bart De Win and Sebastien Deleersnyder
12.30	Talk	The Seven Deadly Sins of SAMM	John Wood
13.00	Roundtable	Agile Guidance for SAMM	Rob van der Veer
14.00	Break		
14.15	Talk	SAMM 2.0 Dashboard	Sathish Ashwin
14.45	Talk	OWASP Top 10 Maturity Categories for Security Champions	Lucian Corlan
15.15	Talk	Using OWASP SAMM to kickstart the SSDLC - Lessons learned from real-world projects	Thomas Kerbl
15.45	Talk	OWASP SAMM: Tools of the Trade	John Ellingsworth
16.15	Break		
16.30	Talk	Lean security: a framework for activities and design factors in DevSecOps	Dennis Verslegers
17.00	Talk	Content Security in Federated Media Cloud Workflows	Ben Schofield
17.30	Talk	Integrating SAMM v2 into Consulting Assessments	Tony Cargile
18.00	Break		
18.15	Workshop	SAMM benchmark - design and user stories	Brian Glas
19.15	Talk	Contributing to SAMM	Patricia Duarte
19.45	Talk	Wrapping up our first SAMM User Day	Bart De Win

OWASP SAMM outreach 2020

Using our social media, sponsor and subscriber networks:

- Twitter - 900 followers
- LinkedIn - 120 followers
- Newsletter - 600+ subscribers
- OWASP SAMM - 8 Sponsors
- SAMM Slack channel - 400+ members



OWASP SAMM

Wrap-up

SAMM User Day

June 16th, 2020

Bart De Win, Seba Deleersnyder

New website 2020

Looking at the impact of our new website compared to 2019:

- Website visitors are staying for longer (up 16%), viewing more pages (up 29%) and returning more often
- With 15,000+ users (up 134%) viewing 120,000+ pages (up 220%) they are viewing more pages per user session
- The #1 source country for visitors is USA (up 137%), with India and the UK growing their contribution in 2nd and 3rd place
- Over half of all website visitors are referrals from OWASP.org (up 155%)

News / Become involved

- Website <https://owaspsamm.org/>
- Github <https://github.com/OWASP/samm/>
- Slack #project-samm, invite <https://owasp-slack.herokuapp.com>
- Newsletter (Mailchimp) <http://eepurl.com/gl9fb9>
- LinkedIn <https://www.linkedin.com/company/owasp-samm>
- Twitter <https://twitter.com/OwaspSAMM>
- YouTube https://www.youtube.com/channel/UCEZDbvQrj5APg5cEET49A_g

Let's do this together



Improve our next User Day

Give us your feedback

3-min survey:

<https://www.surveymonkey.com/r/3NFB35T>



Thank you!