



OWASP SAMM Update

SAMM User Day

May 27th, 2021

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.

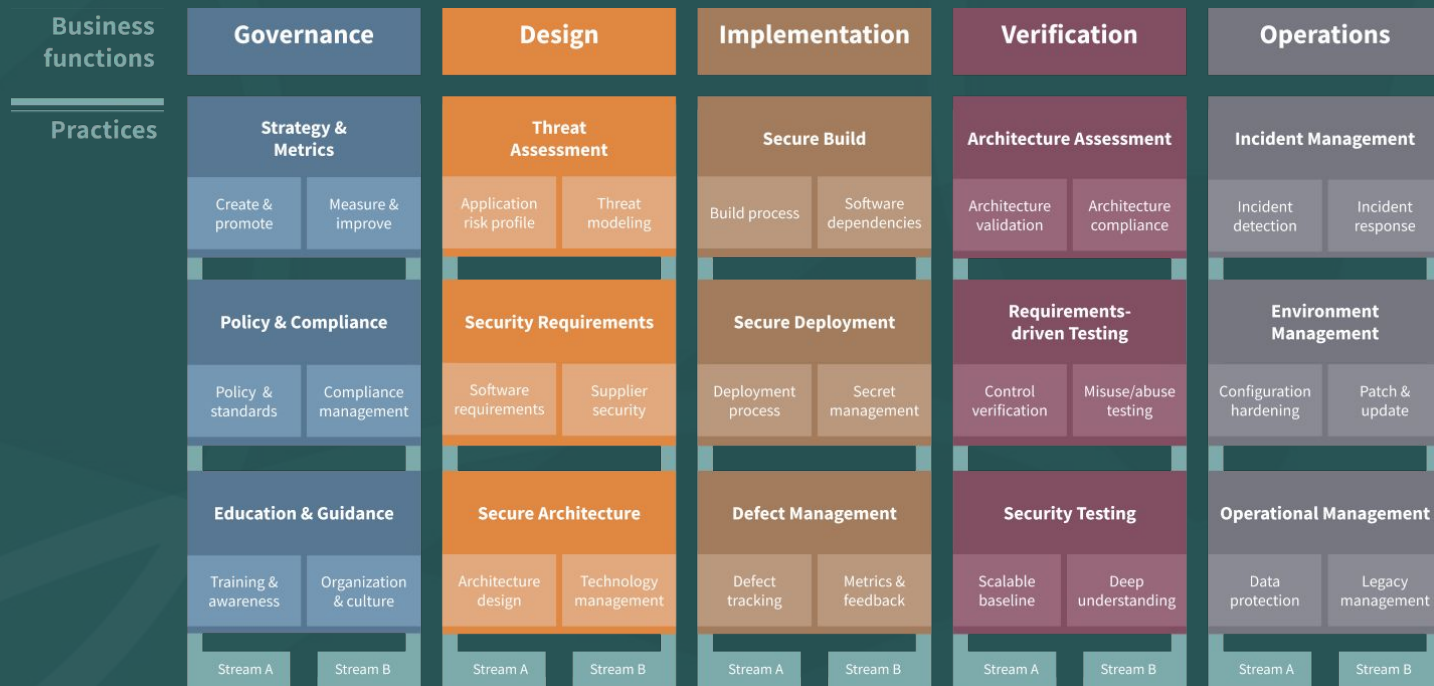


Visit our website

owaspsamm.org



Core structure



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

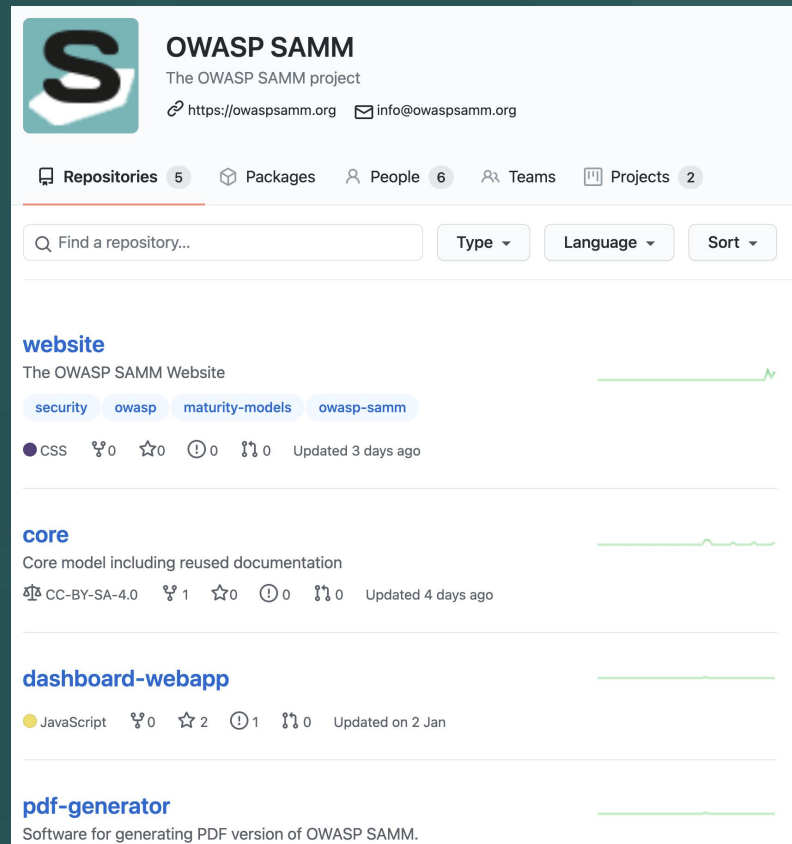
Guidance, references, supporting tools

Community
feedback

SAMM “Suite”

- New GitHub organization
- Loosely coupled subprojects

...more details later on today!



The screenshot shows the GitHub organization page for OWASP SAMM. At the top, the organization name "OWASP SAMM" is displayed with the tagline "The OWASP SAMM project" and contact information: "https://owaspsamm.org" and "info@owaspsamm.org". Below this, navigation tabs show "Repositories" (5), "Packages", "People" (6), "Teams", and "Projects" (2). A search bar is present with the placeholder "Find a repository...". The main content area lists four repositories: "website" (The OWASP SAMM Website, updated 3 days ago), "core" (Core model including reused documentation, updated 4 days ago), "dashboard-webapp" (JavaScript, updated on 2 Jan), and "pdf-generator" (Software for generating PDF version of OWASP SAMM). Each repository entry includes a progress bar and icons for CSS, forks, stars, issues, and pull requests.

OWASP SAMM
The OWASP SAMM project
🔗 <https://owaspsamm.org> ✉ info@owaspsamm.org

📦 Repositories 5 📦 Packages 👤 People 6 👥 Teams 📁 Projects 2

🔍 Find a repository... Type Language Sort

website
The OWASP SAMM Website
security owasp maturity-models owasp-samm
● CSS 🍴 0 ☆ 0 ⌚ 0 🐞 0 Updated 3 days ago

core
Core model including reused documentation
📄 CC-BY-SA-4.0 🍴 1 ☆ 0 ⌚ 0 🐞 0 Updated 4 days ago

dashboard-webapp
JavaScript 🍴 0 ☆ 2 ⌚ 1 🐞 0 Updated on 2 Jan

pdf-generator
Software for generating PDF version of OWASP SAMM.

Translations

Localization management

crowdin.com/project/owasp-samm



Spanish	Juan Calderón
Portuguese	Hugo Fumero
Brazilian Portuguese	Raphael Hagi
German	Tanja Noll
French	Romuald Szkudlarek
Turkish	Ender Akbas
Chinese	Wang Ji
Indonesian	Ade Yoseman
Japanese	Riotaro Okada

Translations

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

THE MODEL



SAMM model overview

Governance	Design	Implementation	Verification	Operations
Strategy and Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy and Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education and Guidance	Security Architecture	Defect Management	Security Testing	Operational Management

Introduction

The mission of OWASP Software Assurance Maturity Model (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 evolvable and risk-driven in nature.

The original model (v1.0) was written by Pravir Chandra and dates back from 2009. Over the last 10 years, it has proven a widely distributed and effective model for improving secure software practices in different types of organizations throughout the world. Translations and supporting tools have been contributed by the community to facilitate adoption and alignment. With version 2.0, we further improve the model to deal with some of its current limitations.

After a period of intensive discussions and with input from practitioners and the OWASP community during summits in Europe and the US on the best way forward, we take a new approach for version 2.0 based on the input we gathered.

For an overview of the version 2 changes, read our [SAMM version 2 release notes](#).

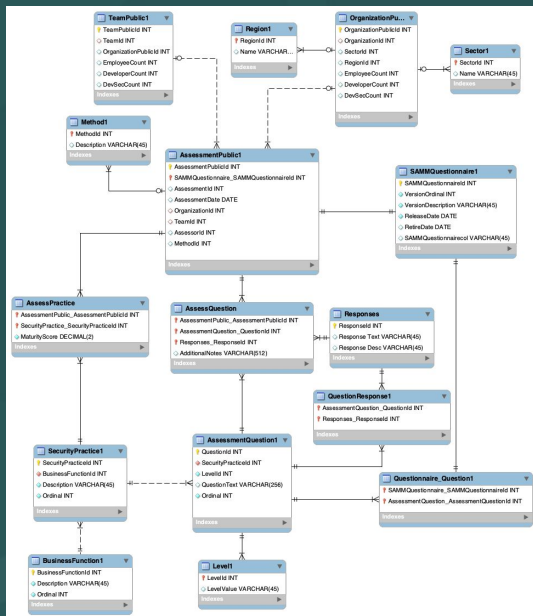
We generated a bare-bones [PDF version](#) of the model. We'll continue to work on it to have a final version as soon as possible.

The screenshot shows a web browser displaying the OWASP SAMM translation tool. The browser's address bar shows the URL: crowdin.com/translate/owasp-samm/12/en-es. The page title is "ACTIVITY G-SM-1-A-YML". The interface is in Spanish. On the left, there is a list of source strings with their IDs. On the right, there is a text area for the translation. Below the text area, there is a "SOURCE STRING" section with a description of the SAMM model. On the far right, there is a "COMMENTS" section with a search bar and a list of comments. The comments are in Turkish and discuss the meaning of "driver" and "factor".

SAMM training grant

- Grant from Motorola Solutions, Inc.
- Creation of a Two-day Train-the-Trainer class
 - Audience: Potential instructors for SAMM Overview class
- Deliverables:
 - Materials and trainer notes for Train-the-Trainer class
 - Improved notes handout for Overview class students
 - Improved Trainer Notes for Overview class presenters
- “Beta Test”: One class, presented live online to MSI staff
 - Use feedback from session to improve content

SAMM benchmarking



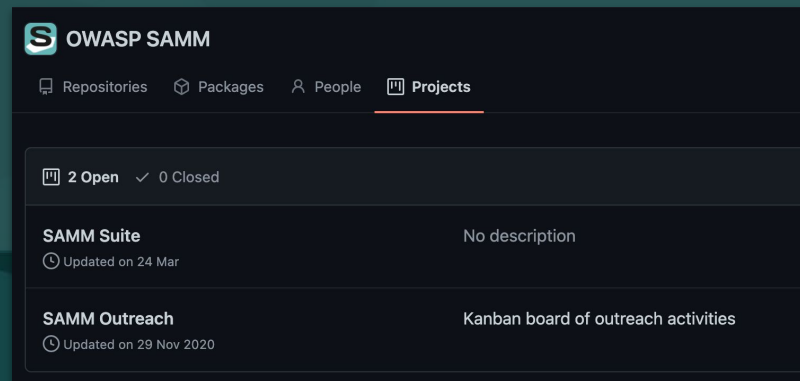
- How do I compare?
- What works for similar organizations?
- Updating the data model for 1.5-2.x
- Trending and population visualizations
- Integration with online assessment
- Work scheduled during this summer
- Please donate SAMM data sets!
- Have cycles? Join this track!

brian.glas@owasp.org
owaspsamm.org/benchmarking



Our roadmap

- Continuous: minor fixes
- Wrap-up: PDF
- v2.1 (ongoing): Translations, mappings
- v2.2 (Fall 2021): Activity-specific guidance (references, agile, ...)
- V2.3 (2022): online toolbox, open API
- V3.0: tbd



Let's do this together



SAMM project leaders



Bart De Win



Sebastien (Seba)
Deleersnyder

The SAMM core team



Sebastián Arriada



Nessim Kisserli



Daniel Kefer



John DiLeo



John Kennedy



Brett Crowley
Chris Cooper



Patricia Duarte



Brian Glas
Yan Kravchenko
Hardik Parekh
John Ellingsworth

Who is SAMM?

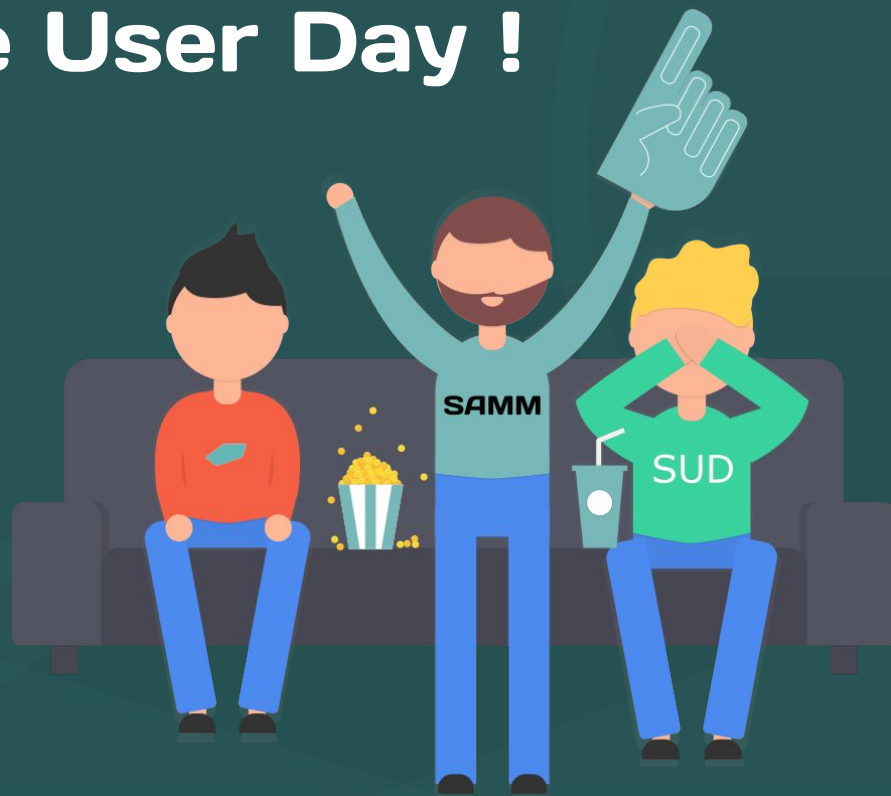
Bart De Win Project Co-Leader, Belgium	Sebastien (Seba) Deleersnyder Project Co-Leader, Belgium
Brian Glasco – United States	Daniel Kefer – Germany
Yan Kravchenko – United States	Chris Cooper – United Kingdom
John DiLeo – New Zealand	Nessim Kisserli – Belgium
Patricia Duarte – Uruguay	John Kennedy –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

SAMM Sponsors



owasp samm.org/sponsors

Enjoy the User Day !



12.00	OWASP SAMM Update	Bart De Win, Sebastien Deleersnyder
12.25	Strategic Usage of OWASP SAMM and OWASP DSOMM	Timo Pagel
12.50 - BREAK		
13.00	WORKSHOP - What should be the organizational scope of an OWASP SAMM assessment?	Carsten Huth
13.50 - BREAK		
14.00	From SAMM Project towards SAMM Suite	Daniel Kefer
14.25	Implementation of SAMM in K12 Schools	Deveeshree Nayak
14.50 - BREAK		
15.00	OWASP SAMM to the rescue? On the intricate challenges of setting up a secure CI/CD pipeline	Asier Rivera Fernandez, Nessim Kisserli
15.50	Wrap-up	Bart De Win, Sebastien Deleersnyder

News / Become involved

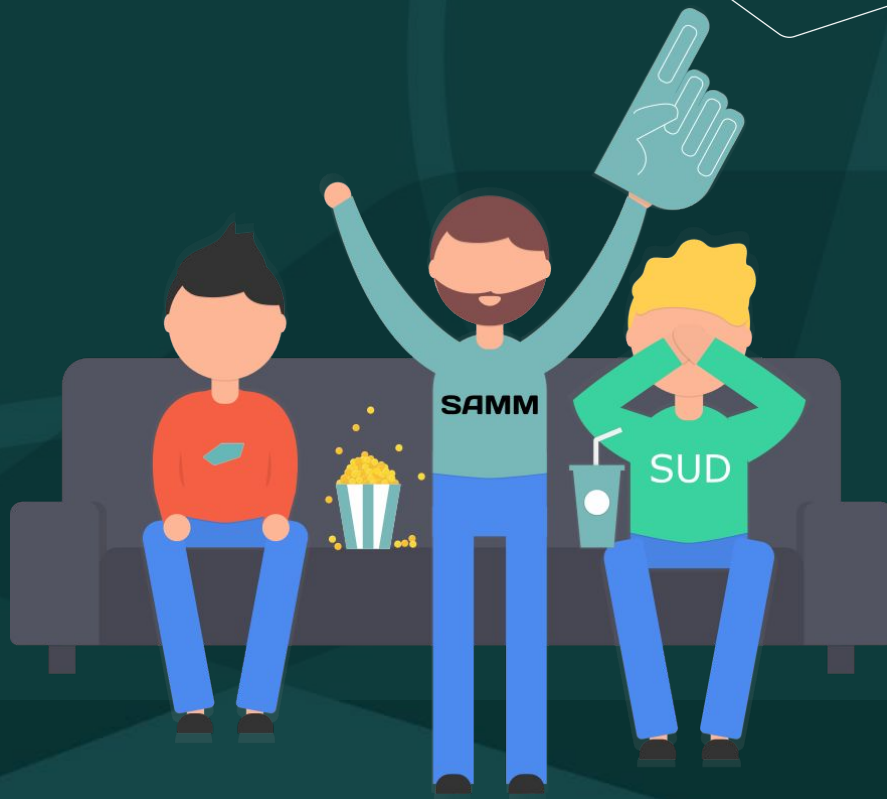
- Monthly community calls each 2dn Wednesday of the month
- Website <https://owaspsamm.org/>
- Github <https://github.com/OWASP samm> - New!
- Slack #project-samm OWASP invitation <https://owasp-slack.herokuapp.com>
- Newsletter (Mailchimp) <http://eepurl.com/gl9fb9>
- Twitter <https://twitter.com/OwaspSamm>
- LinkedIn <https://www.linkedin.com/company/owasp-samm>



Thank you!



Spring User Day





**Autumn
User Day!!!**

10-minute break



13.00	WORKSHOP - What should be the organizational scope of an OWASP SAMM assessment?	Carsten Huth
13.50 - BREAK		
14.00	From SAMM Project towards SAMM Suite	Daniel Kefer
14.25	Implementation of SAMM in K12 Schools	Deveeshree Nayak
14.50 - BREAK		
15.00	OWASP SAMM to the rescue? On the intricate challenges of setting up a secure CI/CD pipeline	Asier Rivera Fernandez, Nessim Kisserli
15.50	Wrap-up	Bart De Win, Sebastien Deleersnyder

10-minute break



14.00	From SAMM Project towards SAMM Suite	Daniel Kefer
14.25	Implementation of SAMM in K12 Schools	Deveeshree Nayak
14.50 - BREAK		
15.00	OWASP SAMM to the rescue? On the intricate challenges of setting up a secure CI/CD pipeline	Asier Rivera Fernandez, Nessim Kisserli
15.50	Wrap-up	Bart De Win, Sebastien Deleersnyder

10-minute break



15.00	OWASP SAMM to the rescue? On the intricate challenges of setting up a secure CI/CD pipeline	Asier Rivera Fernandez, Nessim Kisserli
15.50	Wrap-up	Bart De Win, Sebastien Deleersnyder