OWASP
Open Web Application
Security Project

OWASP SAMM

OWASP SAMM version 2.0

OWASP - New Zealand

Friday, February 21, 2020

John Ellingsworth

johnellingsworth.com

United States Resident

Temple University (BA), Drexel University (MS)

20+ years cybersecurity & web technology experience:

Startups (1996-2000), Higher Education (1999-2009), Corporate (2009-Present): Software Development / Architecture / Security / Management

OWASP: Maine Chapter lead, SAMM Project

Infragard, ASCP

What is SAMM?

The Software Assurance Maturity Model (SAMM) is an open framework that provides an effective and measurable way for all types of organizations to analyze and improve their software security posture.

owaspsamm.org

Measurable
Defined maturity levels across business practices

Actionable
Clear pathways for improving maturity levels

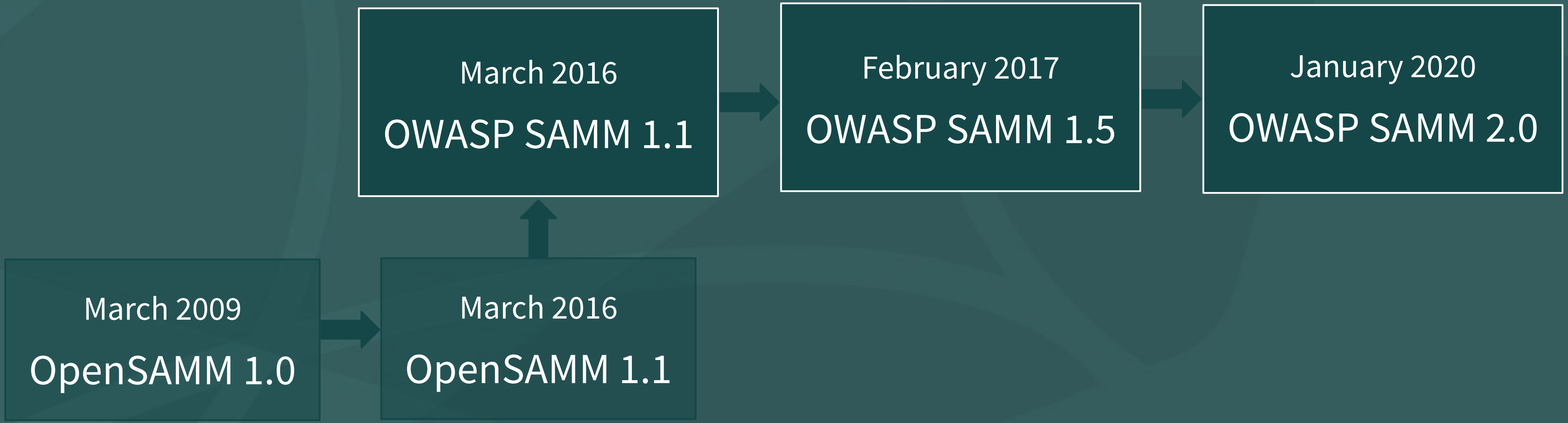
Versatile
Technology, process, and organization agnostic

What is SAMM?

The resources provided by SAMM aid in

- evaluating an organization’s existing software security practices
- building a balanced software security assurance program in well-defined iterations
- demonstrating concrete improvements to a security assurance program
- defining and measuring security-related activities throughout an organization

Project history



March 2009

OpenSAMM 1.0

March 2016

OpenSAMM 1.1

March 2016

OWASP SAMM 1.1

February 2017

OWASP SAMM 1.5

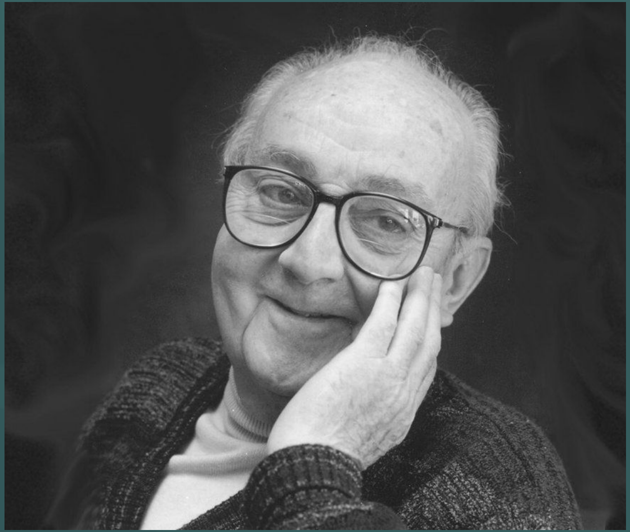
January 2020

OWASP SAMM 2.0

Why SAMM?

"The most that can be expected from any model is that it can supply a useful approximation to reality. All models are wrong; some models are useful."

George E. P. Box



SAMM principles

An organization's behavior changes slowly over time	Changes must be **iterative** while working toward long-term goals
There is no single recipe that works for all organizations	A solution must enable **risk-based** choices tailored to the organization
Guidance related to security activities must be prescriptive	A solution must provide enough **details** for non-security-people
Overall, it must be simple, well-defined, and measurable	OWASP Software Assurance Maturity Model (SAMM)

Maturity levels and scoring

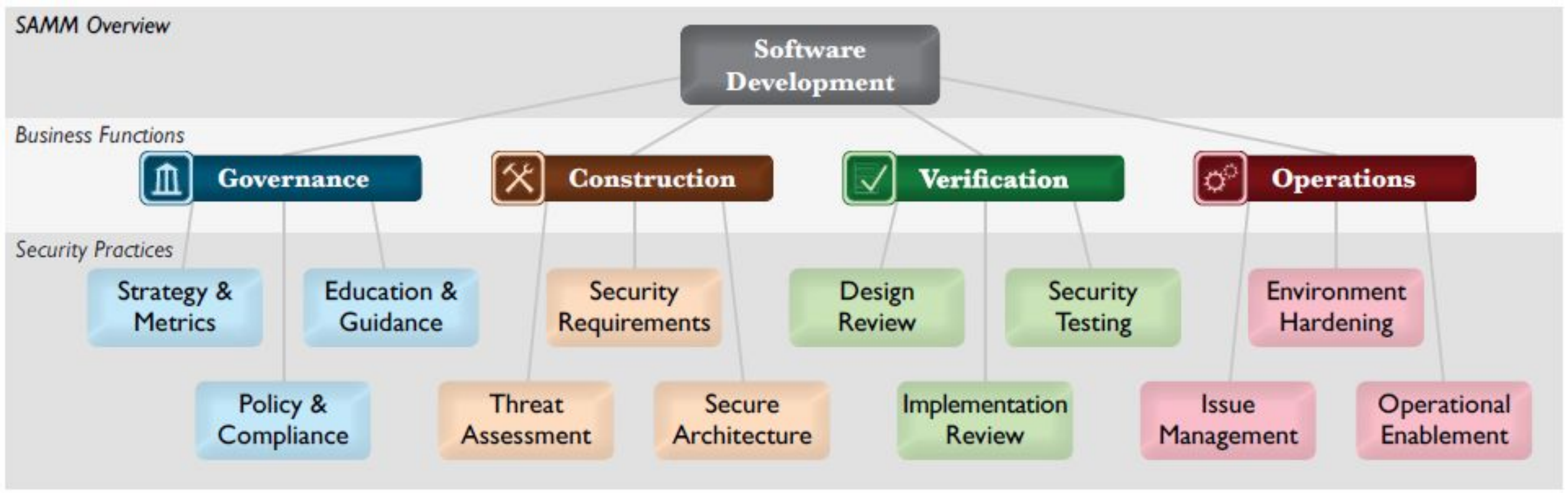
- Transparent view over different levels
- Fine-grained improvements are visible

Maturity levels		Assessment scores	
3	Comprehensive mastery at scale	1	Most
2	Increased efficiency and effectiveness	0.5	At least half
1	Ad-hoc provision	0.2	Some
0	Practice unfulfilled	0	None

SAMM versions 1.5 and 2.0

- Business functions (4 in SAMM 1.5, 5 in SAMM 2.0)
- 3 security practices for each business function
- The security practices cover areas relevant to software security assurance

SAMM 1.5



SAMM Overview

Software Development

Business Functions

Governance

Construction

Verification

Operations

Security Practices

Strategy & Metrics

Policy & Compliance

Education & Guidance

Threat Assessment

Security Requirements

Secure Architecture

Design Review

Implementation Review

Security Testing

Issue Management

Environment Hardening

Operational Enablement

OWASP
Open Web Application
Security Project

SAMM 2.0

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

SAMM 2.0

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

OWASP
Open Web Application
Security Project

Governance		Design		Implementation		Verification		Operations	
Strategy & Metrics		Threat Assessment		Secure Build		Architecture Assessment		Incident Management	
Create & promote	Measure & improve	App risk profile	Threat model	Build process	Dependencies	Architecture validation	Architecture compliance	Incident detection	Incident response
Policy & Compliance		Security Requirements		Secure Deployment		Requirements-driven Testing		Environment Management	
Policy & standards	Compliance mgmt	Software reqmts	Supplier security	Deployment process	Secret mgmt	Control verification	Misuse/abuse testing	Config hardening	Patch & update
Education & Guidance		Secure Architecture		Defect Management		Security Testing		Operational Management	
Training & awareness	Org & culture	Architecture design	Technology mgmt	Defect tracking	Metrics & feedback	Scalable baseline	Deep understanding	Data protection	Legacy mgmt
Stream A	Stream B	Stream A	Stream B	Stream A	Stream B	Stream A	Stream B	Stream A	Stream B

Governance		Design		Implementation		Verification		Operations	
Strategy & Metrics		**Threat Assessment**		**Secure Build**		**Architecture Assessment**		**Incident Management**	
Create & promote	Measure & improve	App risk profile	Threat model	Build process	Dependencies	Architecture validation	Architecture compliance	Incident detection	Incident response
Policy & Compliance		**Security Requirements**		**Secure Deployment**		**Requirements-driven Testing**		**Environment Management**	
Policy & standards	Compliance mgmt	Software reqmts	Supplier security	Deployment process	Secret mgmt	Control verification	Misuse/abuse testing	Config hardening	Patch & update
Education & Guidance		**Secure Architecture**		**Defect Management**		**Security Testing**		**Operational Management**	
Training & awareness	Org & culture	Architecture design	Technology mgmt	Defect tracking	Metrics & feedback	Scalable baseline	Deep understanding	Data protection	Legacy mgmt
Stream A	Stream B	Stream A	Stream B	Stream A	Stream B	Stream A	Stream B	Stream A	Stream B

SAMM v2 assessment toolbox

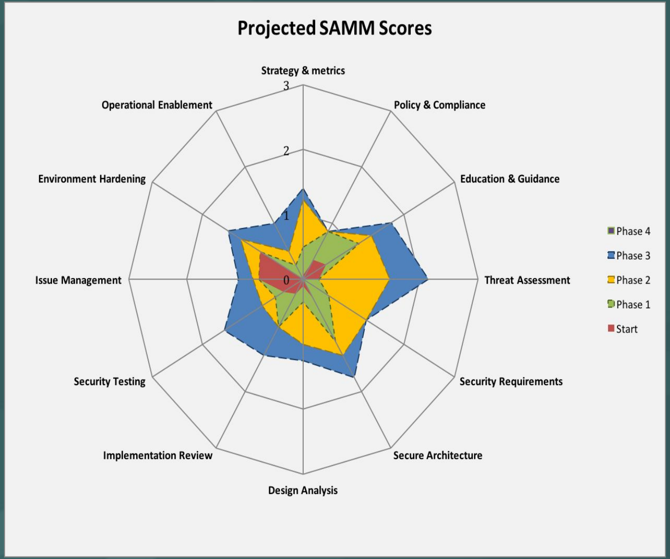
GOVERNANCE		
Stream	**Level**	**Strategy and metrics**
Create and promote	1	Has the organization defined a set of risks to prioritize applications by?
		● You have captured the risk appetite of your organization’s executive leadership ● The organization’s leadership have vetted and approved risks ● You 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

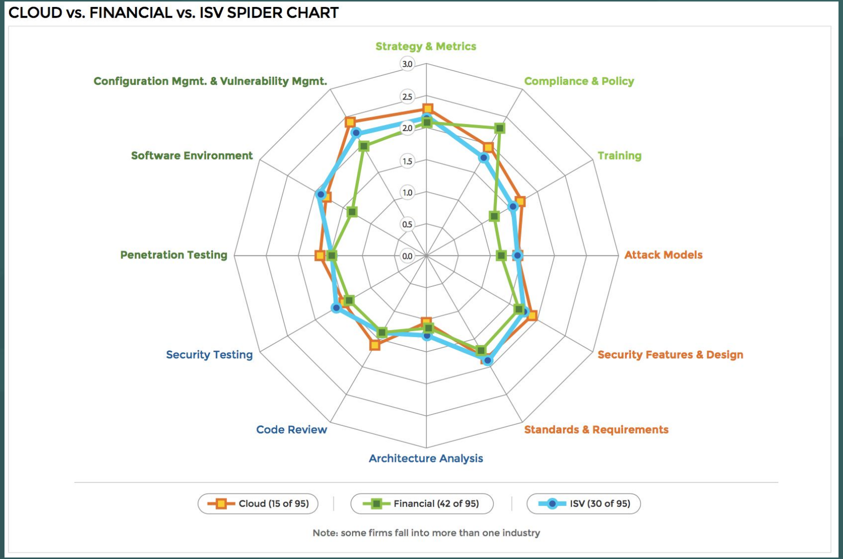
Critical success factors

- Get buy-in from stakeholders
- Adopt a risk-based approach
- Awareness & education are the foundation
- Integrate & automate security in your development, acquisition, and deployment processes
- Measure: provide management visibility

SAMM can (sorta) map to BSIMM



SAMM



BSIMM

Time to answer the question…

How do I compare?

SAMM benchmarking

owaspsamm.org/benchmarking

What is SAMM benchmarking?

The goal of this project is to collect the most comprehensive dataset related to organizational maturity of application or software security programs.

This data should come from both self-assessing organizations and consultancies that perform third party assessments.

Contribution 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 with 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.

Data contributions

Verified data contribution

- the submitter is **known** and has agreed to be **identified** as a contributing party
- the submitter is **known** but would rather **not** be publicly **identified**
- the submitter is **known** but does **not** want it **recorded** in the dataset

Unverified data contribution

- the submitter is **anonymous**

Ways of contributing

Current

- Email a CSV/Excel/Doc file with the dataset(s) to brian.glas@owasp.org

Future

- Upload a CSV/Excel/Txt file to a contribution web page
- Complete the web-based form
- Upload the data from the SAMM Toolbox

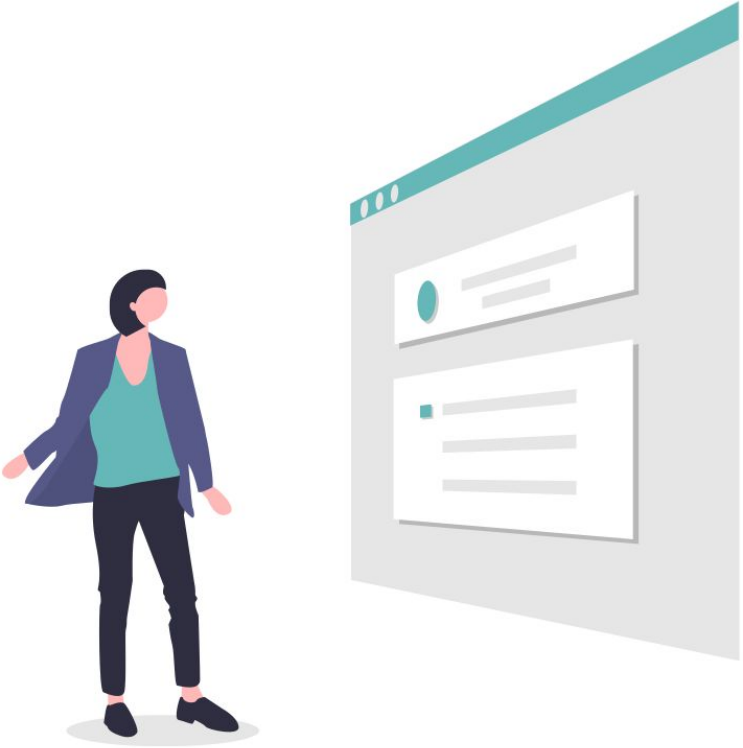
Data structure

- *Contributor Name (org or anon)
- Contributor Contact Email
- *Date assessment conducted (MM/YYYY)
- *Type of Assessment (self or 3rd party)
- *Answers to the SAMM Assessment Questions
- Geographic Region (global, North America, EU, Asia, other)
- Primary Industry (multiple, financial, industrial, software, ??)
- Approximate number of developers (1-100, 101-1000, 1001-10000, 10000+)
- Approximate number of primary AppSec (1-5, 6-10, 11-20, 20+)
- Approximate number of secondary AppSec (0-20, 21-50, 51-100, 100+)
- Primary SDL Methodology (Waterfall, Agile, DevOps, Other)

* required fields

Visit our website

owaspsamm.org



Questions, feedback, input

#project-samm

github.com/OWASP/samm

SAMM newsletter

mailchimp

eepurl.com/gl9fb9

SAMM sponsors

CONCORD
MICRO FOCUS
Fortify
nccgroup
pwc
splunk>
TOREON

owaspsamm.org/sponsors

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

OWASP
Open Web Application
Security Project

OWASP
SAMM

Questions?
Feedback?

OWASP
Open Web Application
Security Project

OWASP
SAMM

Thank you!

john.ellingsworth@owasp.org
john@ellingsworth.org
johnellingsworth.com