OWASP SAMM2 – Your Dynamic Software Security Journey

OWASP Helsinki chapter meeting #39
Tuesday, October 22, 2019

Sebastien Deleersnyder

CEO Toreon

Belgian OWASP chapter founder

SAMM project co-leader

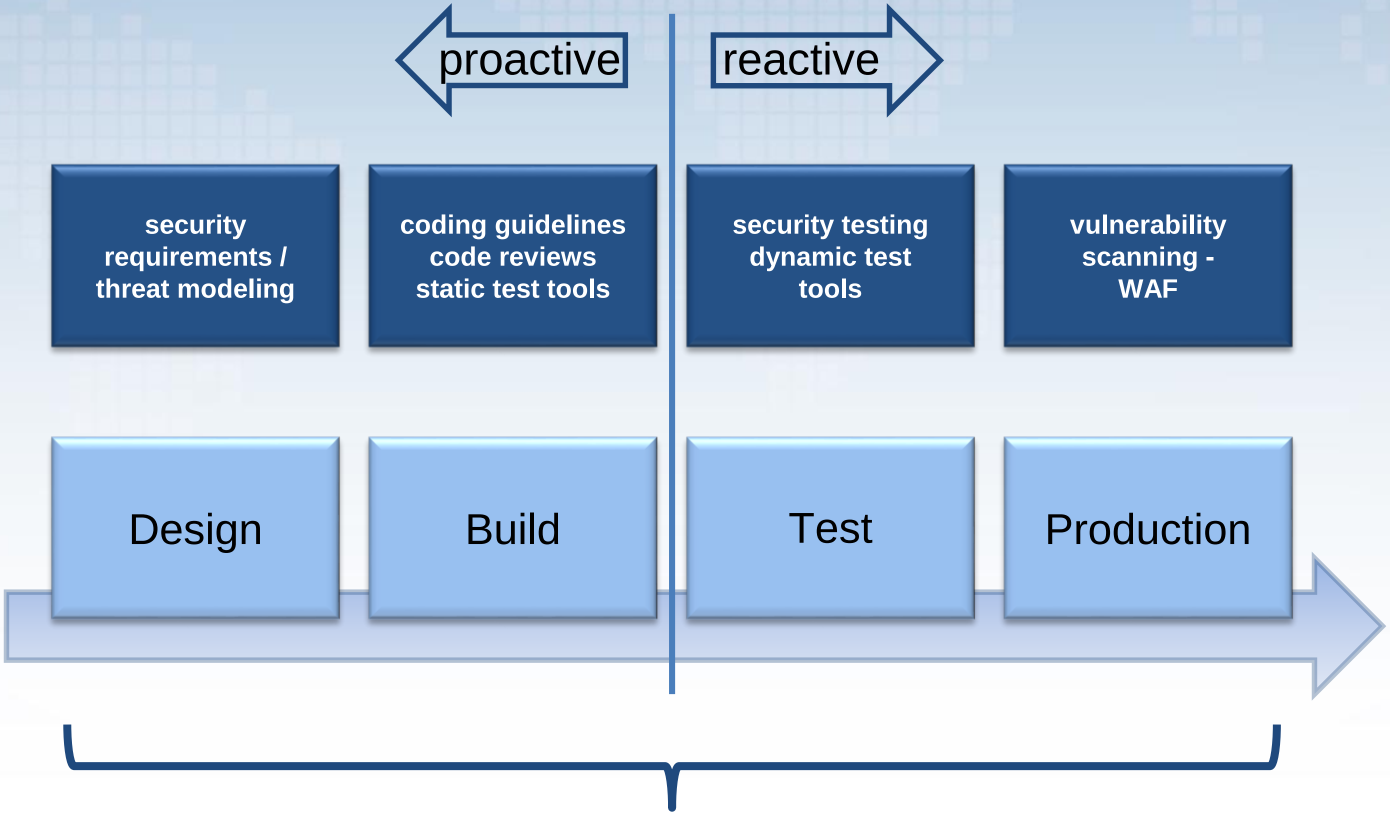
Subscribe to our Threat Modeling Insider newsletter
Guest articles, curated articles, white papers, tips …
http://eepurl.com/ghAr8b

What is SAMM?

FLAGSHIP mature projects

"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.”

“Build in” software assurance



proactive

reactive

security requirements / threat modeling

coding guidelines
code reviews
static test tools

security testing
dynamic test tools

vulnerability scanning - WAF

Design

Build

Test

Production

Secure Development Lifecycle
(SAMM)

Why a maturity model?

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, must be simple, well-defined, and measurable

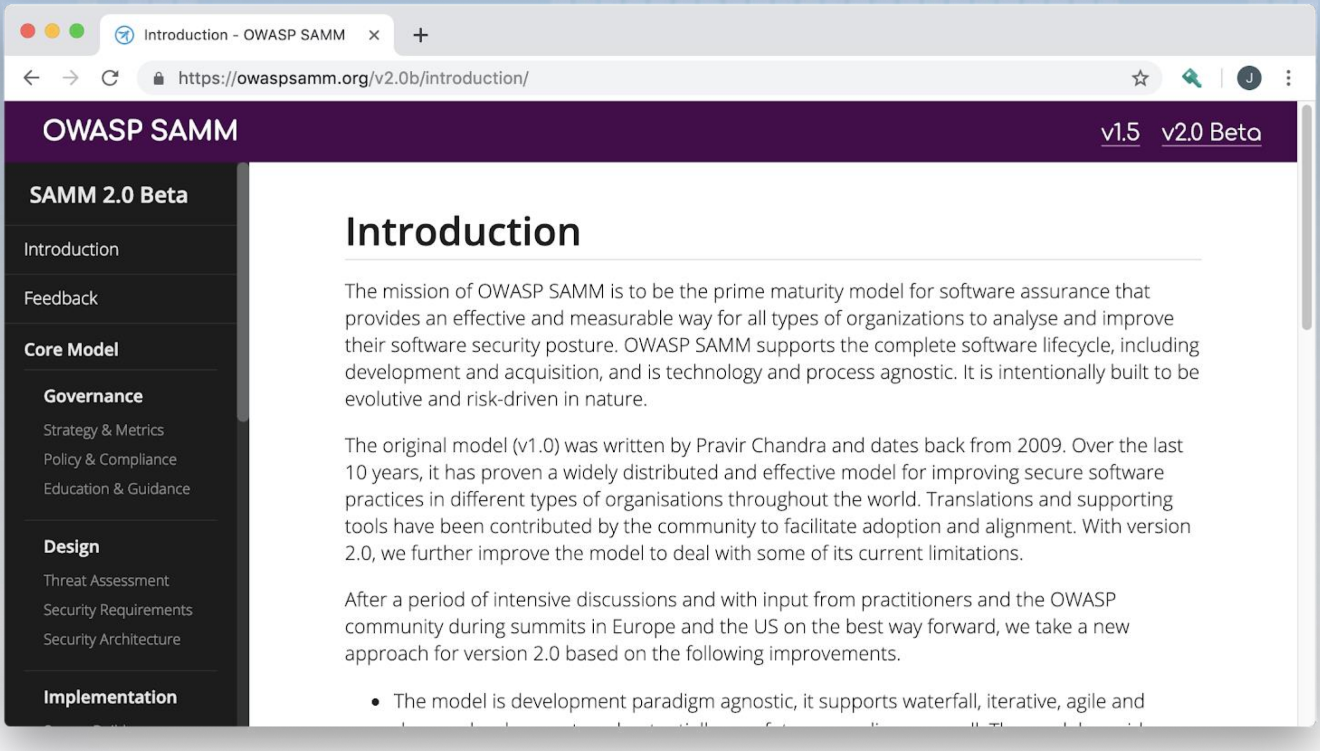
OWASP Software Assurance Maturity Model (SAMM)

Measurable

Actionable

Versatile

OWASP SAMM



Introduction

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 analyse 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.

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 organisations 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.

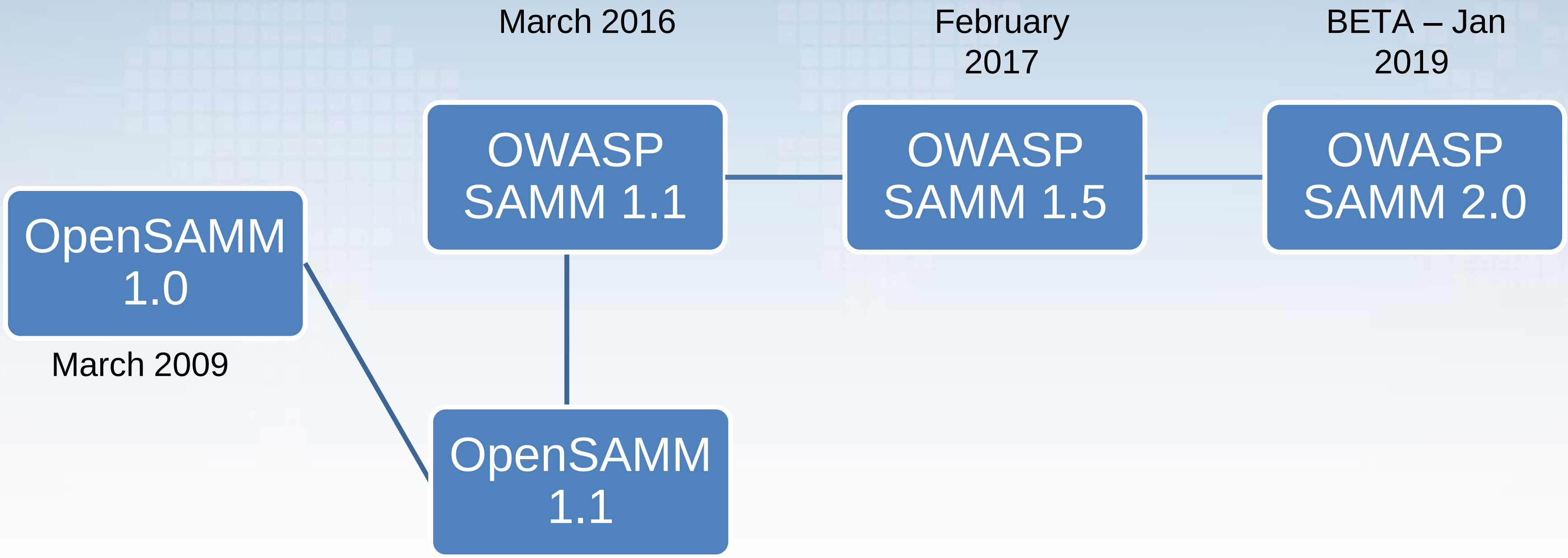
After a period of intensive discussions and with input from practitioners and the OWASP community during summits in Europe and the US on the best way forward, we take a new approach for version 2.0 based on the following improvements.

- The model is development paradigm agnostic, it supports waterfall, iterative, agile and

https://owaspsamm.org/

OWASP
Open Web Application
Security Project

Project History



OpenSAMM 1.0

March 2009

OpenSAMM 1.1

March 2016

OWASP SAMM 1.1

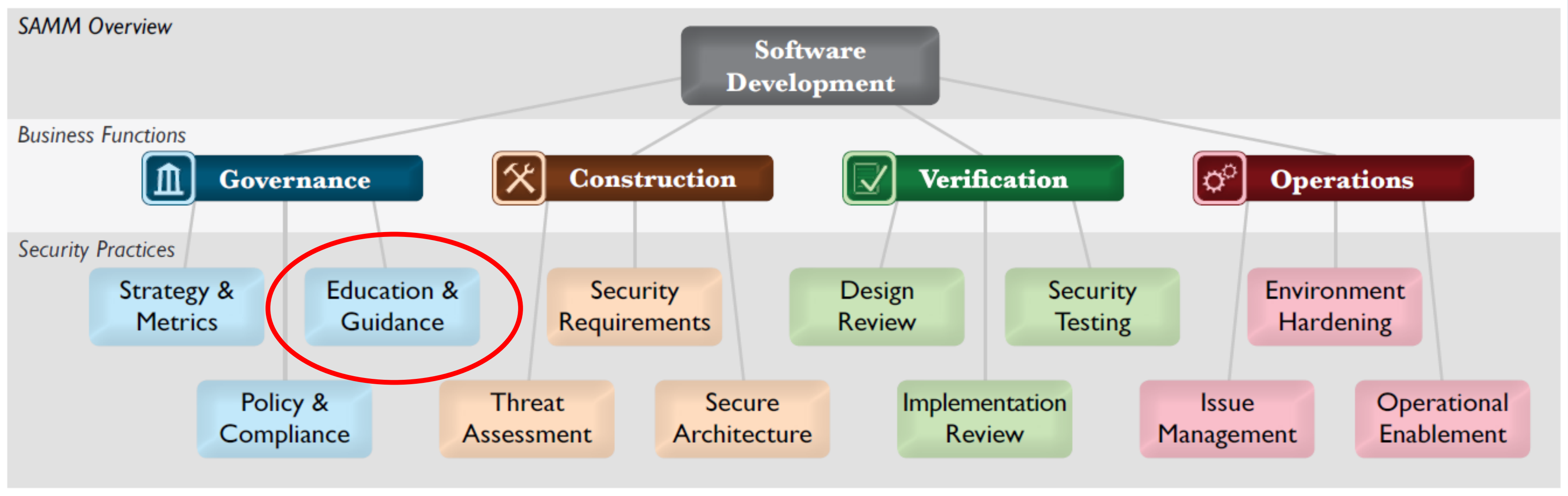
February 2017

OWASP SAMM 1.5

BETA – Jan 2019

OWASP SAMM 2.0

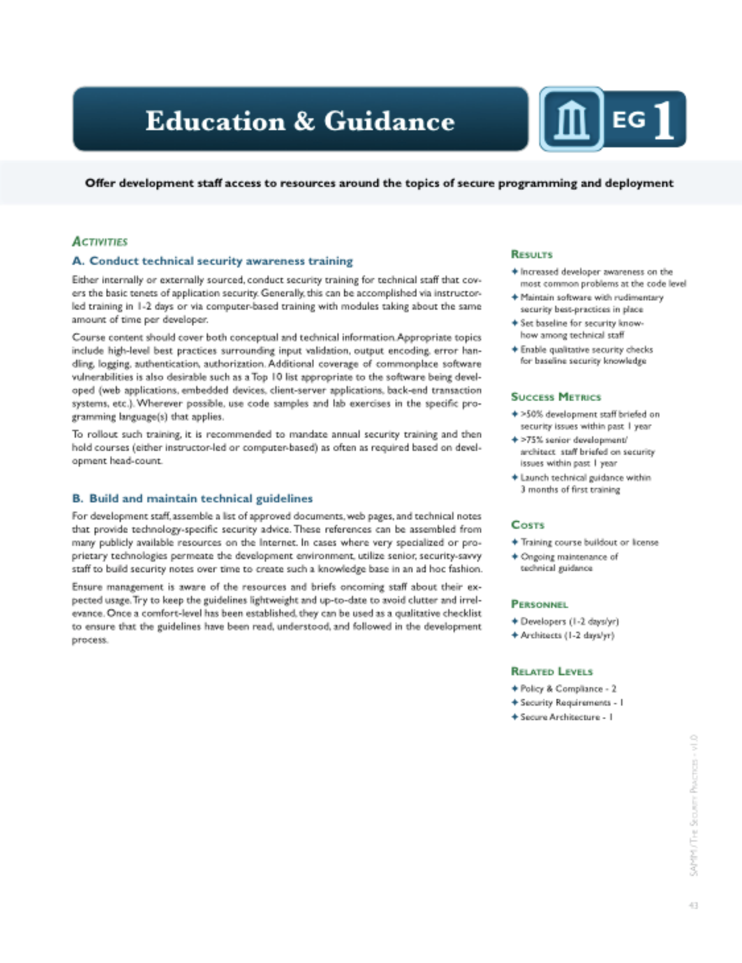
Core structure (v1.5)



OWASP
Open Web Application Security Project

Per Level, SAMM defines…

- Objective
- Activities
- Results
- Success Metrics
- Costs
- Personnel
- Related Levels



Education & Guidance

EG 1

Offer development staff access to resources around the topics of secure programming and deployment

Activities

A. Conduct technical security awareness training

Either internally or externally sourced, conduct security training for technical staff that covers the basic tenets of application security. Generally, this can be accomplished via instructor-led training in 1-2 days or via computer-based training with modules taking about the same amount of time per developer.

Course content should cover both conceptual and technical information. Appropriate topics include high-level best practices surrounding input validation, output encoding, error handling, logging, authentication, authorization. Additional coverage of commonplace software vulnerabilities is also desirable such as a Top 10 list appropriate to the software being developed (web applications, embedded devices, client-server applications, back-end transaction systems, etc.). Wherever possible, use code samples and lab exercises in the specific programming language(s) that applies.

To rollout such training, it is recommended to mandate annual security training and then hold courses (either instructor-led or computer-based) as often as required based on development head-count.

B. Build and maintain technical guidelines

For development staff, assemble a list of approved documents, web pages, and technical notes that provide technology-specific security advice. These references can be assembled from many publicly available resources on the Internet. In cases where very specialized or proprietary technologies permeate the development environment, utilize senior, security-savvy staff to build security notes over time to create such a knowledge base in an ad hoc fashion.

Ensure management is aware of the resources and briefs oncoming staff about their expected usage. Try to keep the guidelines lightweight and up-to-date to avoid clutter and irrelevance. Once a comfort-level has been established, they can be used as a qualitative checklist to ensure that the guidelines have been read, understood, and followed in the development process.

Results

- ✦ Increased developer awareness on the most common problems at the code level
- ✦ Maintain software with rudimentary security best-practices in place
- ✦ Set baseline for security know-how among technical staff
- ✦ Enable qualitative security checks for baseline security knowledge

Success Metrics

- ✦ >50% development staff briefed on security issues within past 1 year
- ✦ >75% senior development/ architect staff briefed on security issues within past 1 year
- ✦ Launch technical guidance within 3 months of first training

Costs

- ✦ Training course buildout or license
- ✦ Ongoing maintenance of technical guidance

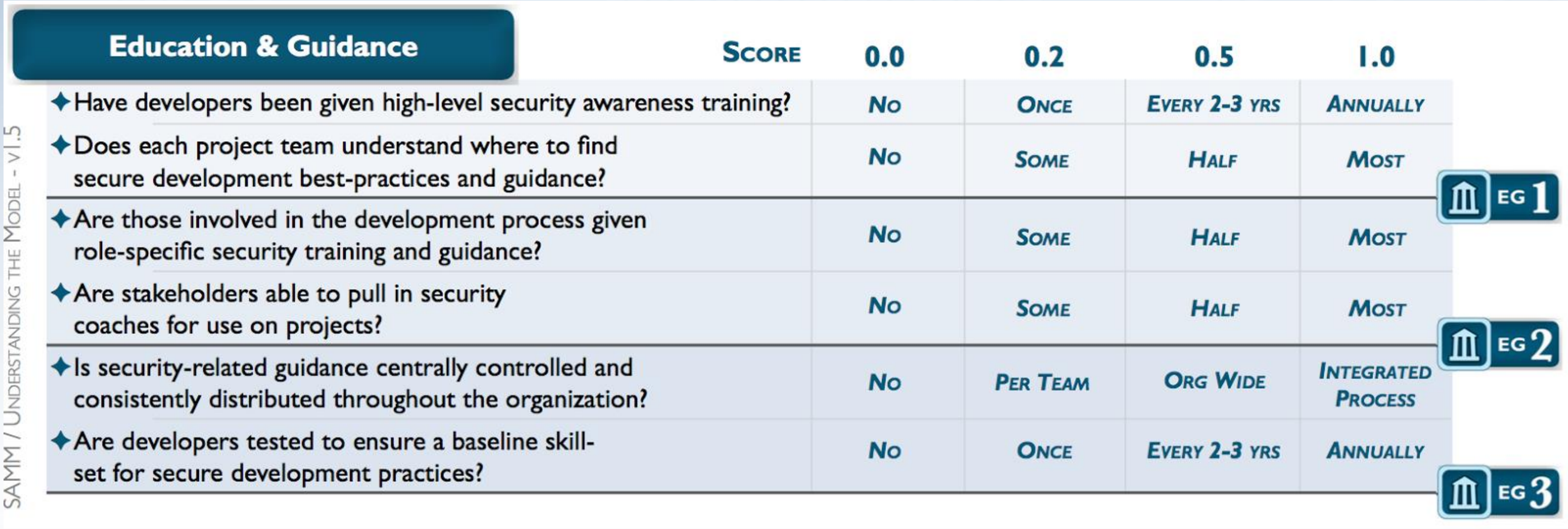
Personnel

- ✦ Developers (1-2 days/yr)
- ✦ Architects (1-2 days/yr)

Related Levels

- ✦ Policy & Compliance - 2
- ✦ Security Requirements - 1
- ✦ Secure Architecture - 1

Assessments

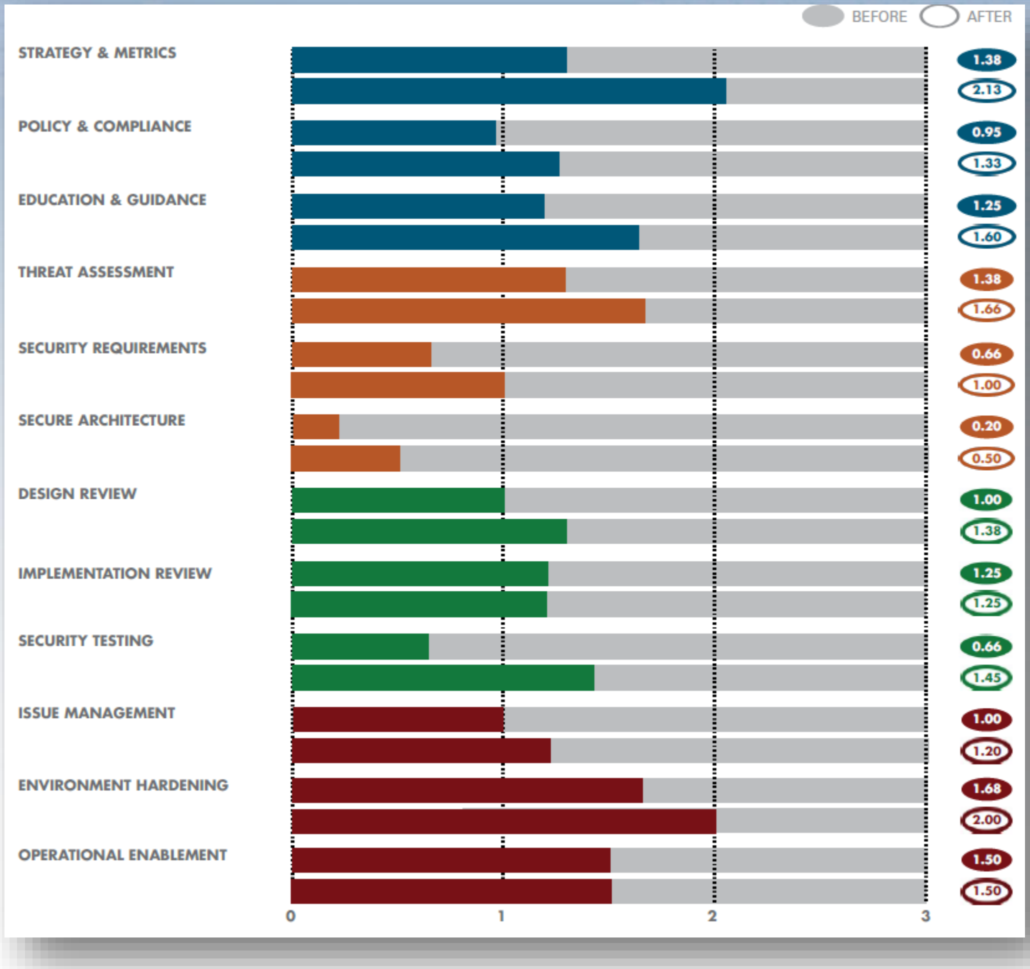


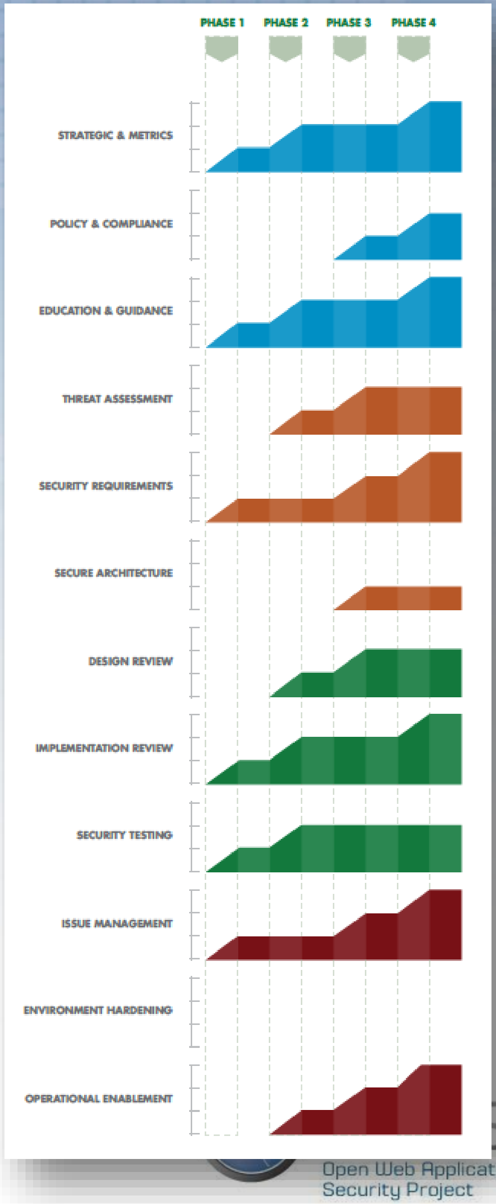
Education & Guidance	Score 0.0	0.2	0.5	1.0	
✦ Have developers been given high-level security awareness training?	No	Once	Every 2-3 yrs	Annually	
✦ Does each project team understand where to find secure development best-practices and guidance?	No	Some	Half	Most	EG 1
✦ Are those involved in the development process given role-specific security training and guidance?	No	Some	Half	Most	
✦ Are stakeholders able to pull in security coaches for use on projects?	No	Some	Half	Most	EG 2
✦ Is security-related guidance centrally controlled and consistently distributed throughout the organization?	No	Per Team	Org Wide	Integrated Process	
✦ Are developers tested to ensure a baseline skill-set for secure development practices?	No	Once	Every 2-3 yrs	Annually	EG 3

SAMM / Understanding the Model - v1.5

OWASP
Open Web Application Security Project

SAMM output


BEFORE
AFTER
STRATEGY & METRICS
1.38
2.13
POLICY & COMPLIANCE
0.95
1.33
EDUCATION & GUIDANCE
1.25
1.60
THREAT ASSESSMENT
1.38
1.66
SECURITY REQUIREMENTS
0.66
1.00
SECURE ARCHITECTURE
0.20
0.50
DESIGN REVIEW
1.00
1.38
IMPLEMENTATION REVIEW
1.25
1.25
SECURITY TESTING
0.66
1.45
ISSUE MANAGEMENT
1.00
1.20
ENVIRONMENT HARDENING
1.68
2.00
OPERATIONAL ENABLEMENT
1.50
1.50
0
1
2
3


PHASE 1
PHASE 2
PHASE 3
PHASE 4
STRATEGIC & METRICS
POLICY & COMPLIANCE
EDUCATION & GUIDANCE
THREAT ASSESSMENT
SECURITY REQUIREMENTS
SECURE ARCHITECTURE
DESIGN REVIEW
IMPLEMENTATION REVIEW
SECURITY TESTING
ISSUE MANAGEMENT
ENVIRONMENT HARDENING
OPERATIONAL ENABLEMENT

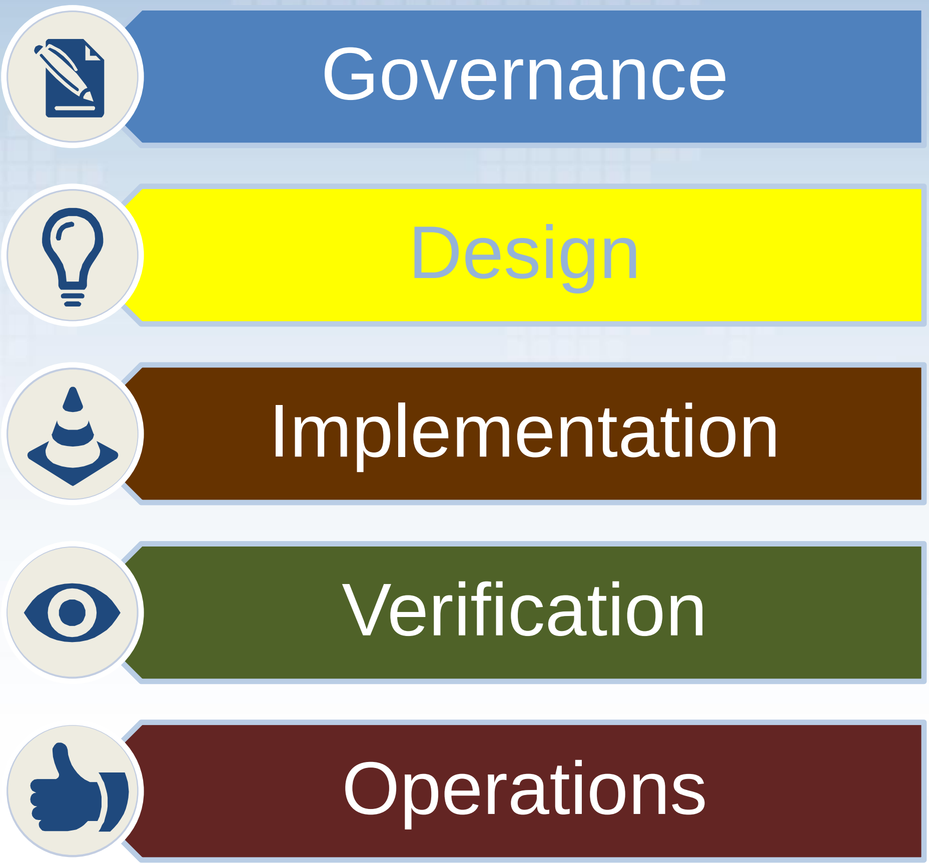
Why a new version?

- ✓Align with recent development practices
- ✓"Orphaned" activities
- ✓Method agnostic
- ✓Improve assessments
- ✓Improve SAMM release process

Backwards compatibility was not a goal

OWASP
Open Web Application
Security Project

SAMM2 business functions



Governance

Design

Implementation

Verification

Operations

OWASP
Open Web Application
Security Project

SAMM2 security practices

- Still 3 Security Practices per Business Function

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

SAMM v2.0 Core Framework

Governance		
Strategy & Metrics	**Create and Promote**	**Measure and Improve**
Policy & Compliance	**Policy and Standards**	**Compliance Management**
Education & Guidance	**Training and Awareness**	**Organization and Culture**
Design		
Threat Assessment	**Application Risk Profile**	**Threat Modeling**
Security Requirements	**Software Requirements**	**Supplier Security**
Secure Architecture	**Architecture Design**	**Technology Management**
Implementation		
Secure Build	**Build Process**	**Software Dependencies**
Secure Deployment	**Deployment Process**	**Secret Management**
Defect Management	**Defect Tracking (Flaws/Bugs/Process)**	**Metrics and Feedback/Learning**
Verification		
Architecture Assessment	**Architecture Validation**	**Architecture Compliance**
Requirements Testing	**Control Verification**	**Misuse/Abuse Testing**
Security Testing	**Scalable Baseline**	**Deep Understanding**
Operations		
Incident Management	**Incident Detection**	**Incident Response**
Environment Management	**Configuration Hardening**	**Patching and Updating**
Operational Management	**Data Protection**	**System decommissioning / Legacy management**

SAMM2 security practice structure
Requirements Testing

Streams

Maturity

Activities

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

OWASP
Open Web Application
Security Project

Scoring in SAMM v1.5

Strategy & Metrics, Level 1: *Is there a software security assurance program in place?*

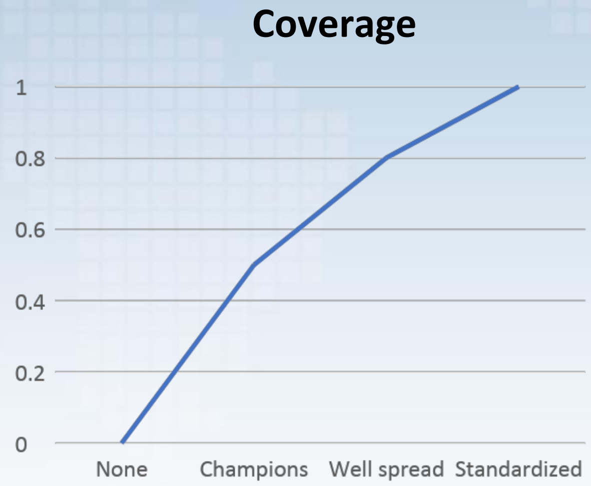
Available Responses:

- *No*
- *Yes, it‘s less than a year old*
- *Yes, it‘s a number of years old*
- *Yes, it‘s a pretty mature program*

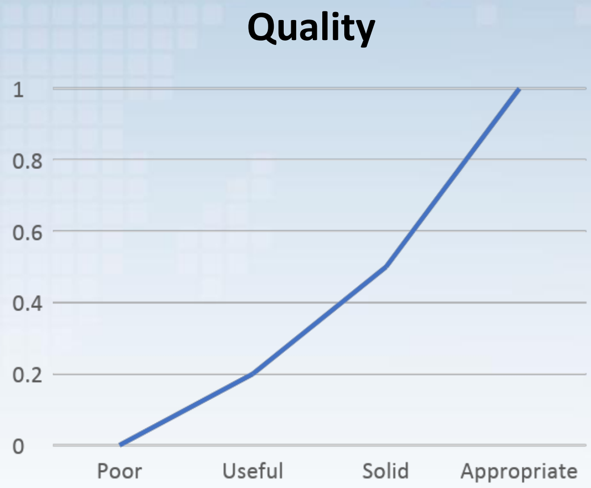
But, what about…

- Quality of the program?
- Freshness of the program? Has it been reviewed/updated?
- How do you know the program is still relevant?

Multiple dimensions to consider

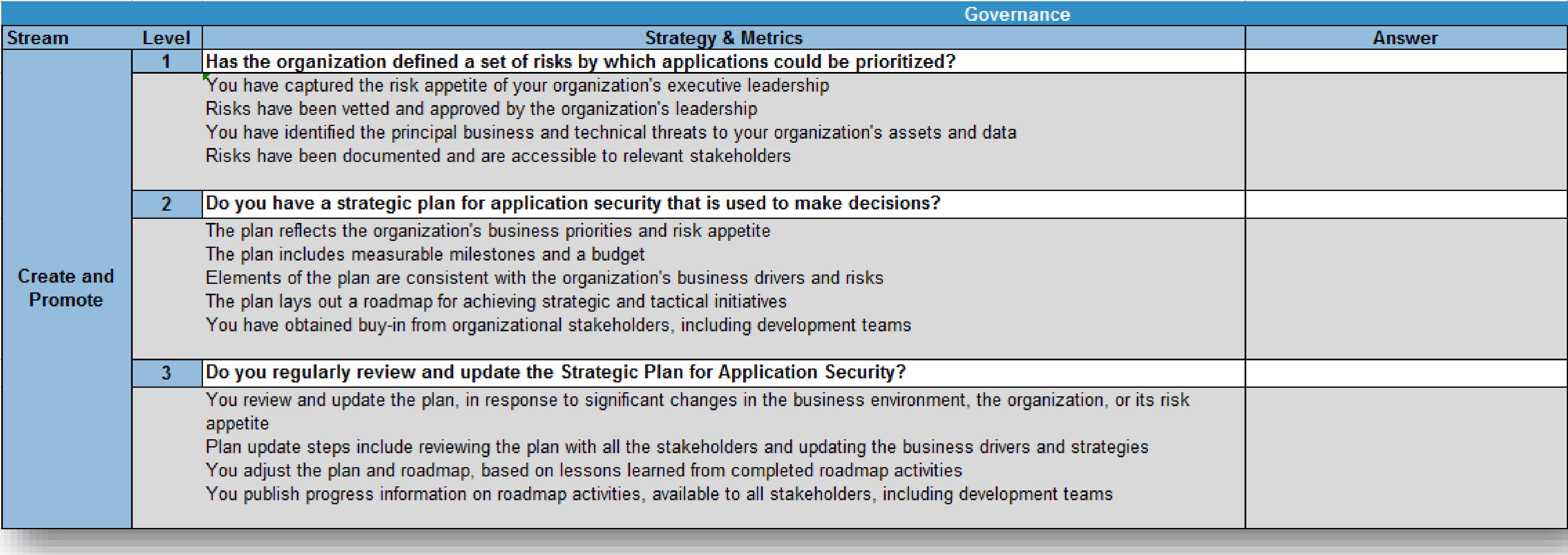


SAMM2:
Questions



SAMM2:
Quality criteria (mandatory)

SAMM2 assessments



		Governance	
Stream	Level	Strategy & Metrics	Answer
Create and Promote	1	**Has the organization defined a set of risks by which applications could be prioritized?**	
		You have captured the risk appetite of your organization's executive leadership Risks have been vetted and approved by the organization's leadership You have identified the principal business and technical threats to your organization's assets and data Risks have been documented and are accessible to relevant stakeholders	
	2	**Do you have a strategic plan for application security that is used to make decisions?**	
		The plan reflects the organization's business priorities and risk appetite The plan includes measurable milestones and a budget Elements of the plan are consistent with the organization's business drivers and risks The plan lays out a roadmap for achieving strategic and tactical initiatives You have obtained buy-in from organizational stakeholders, including development teams	
	3	**Do you regularly review and update the Strategic Plan for Application Security?**	
		You review and update the plan, in response to significant changes in the business environment, the organization, or its risk appetite Plan update steps include reviewing the plan with all the stakeholders and updating the business drivers and strategies You adjust the plan and roadmap, based on lessons learned from completed roadmap activities You publish progress information on roadmap activities, available to all stakeholders, including development teams	

SAMM2 Toolbox:
https://github.com/OWASP/samm/tree/master/Supporting%20Resources/v2.0/toolbox

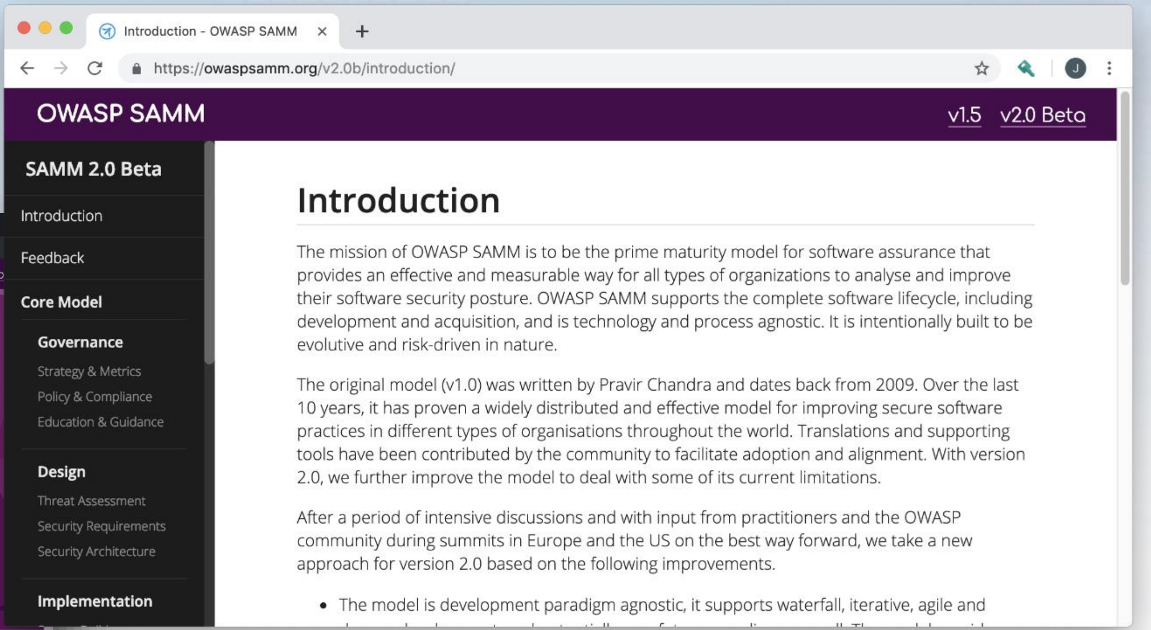
OWASP
Open Web Application Security Project

Owaspsamm.org and toolbox demo

Your organization's dynamic software security strategy

We also maintain a working copy which is updated in real time based on our GitHub respository.

The prime maturity model for software assurance that provides an effective and measurable way for all types of



Introduction

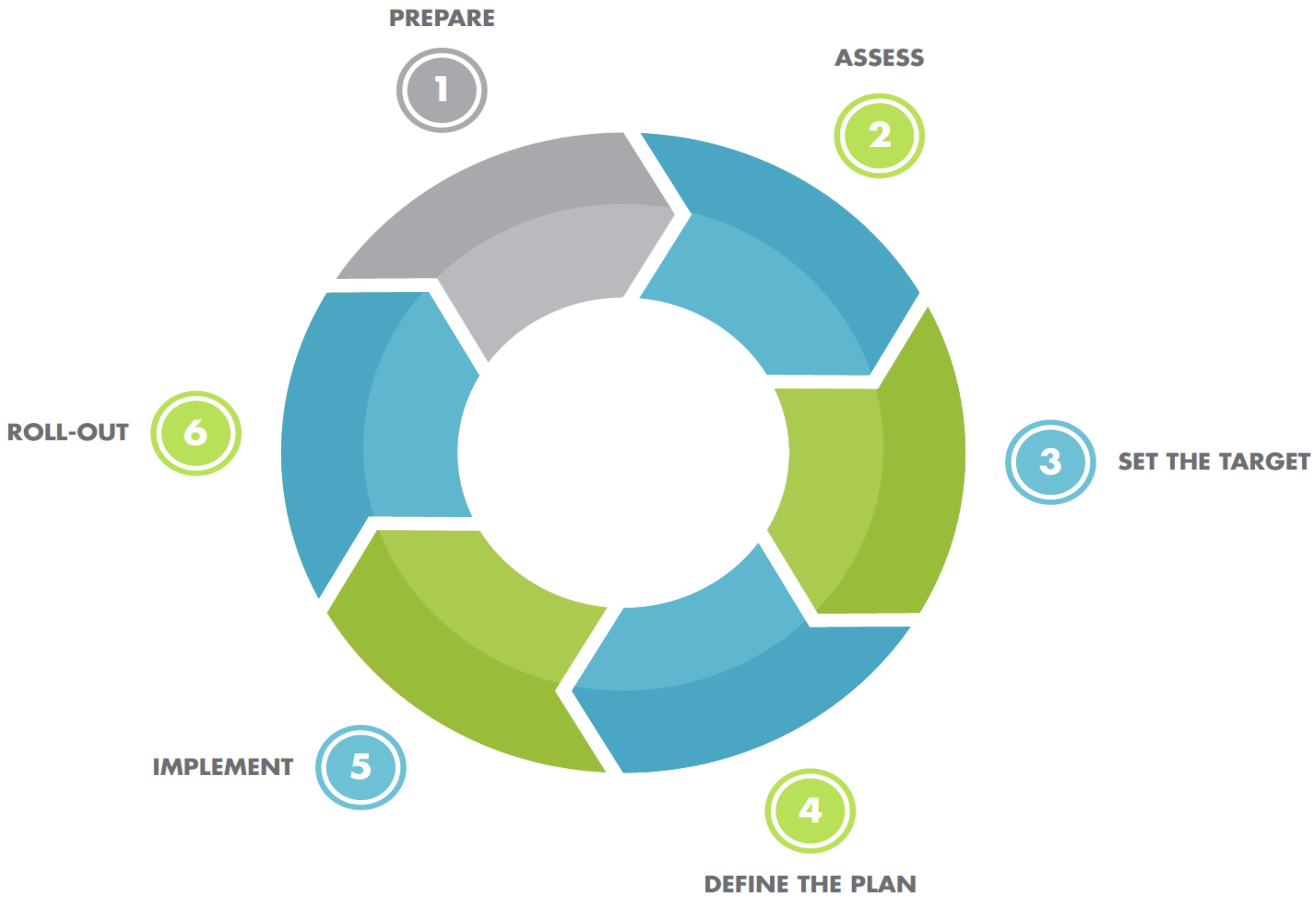
The mission of OWASP SAMM is to be the prime maturity model for software assurance that provides an effective and measurable way for all types of organizations to analyse and improve their software security posture. OWASP SAMM supports the complete software lifecycle, including development and acquisition,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

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 organisations 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 following improvements.

- The model is development paradigm agnostic, it supports waterfall, iterative, agile and

OWASP
Open Web Application Security Project



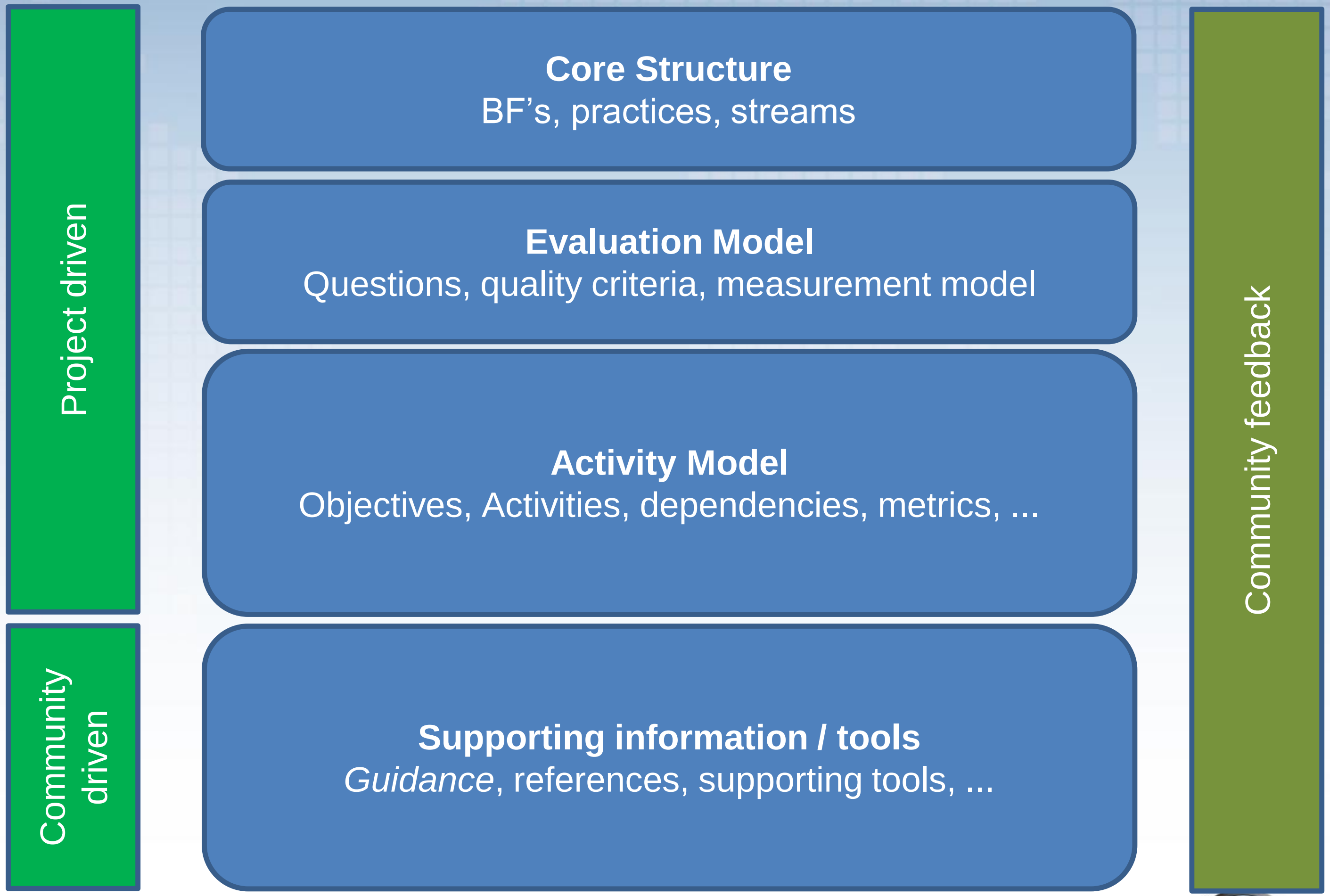
Quick-Start Guide

OWASP
Open Web Application
Security Project

Project: new way of working

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

Community involvement



Project driven

Community driven

Core Structure
BF's, practices, streams

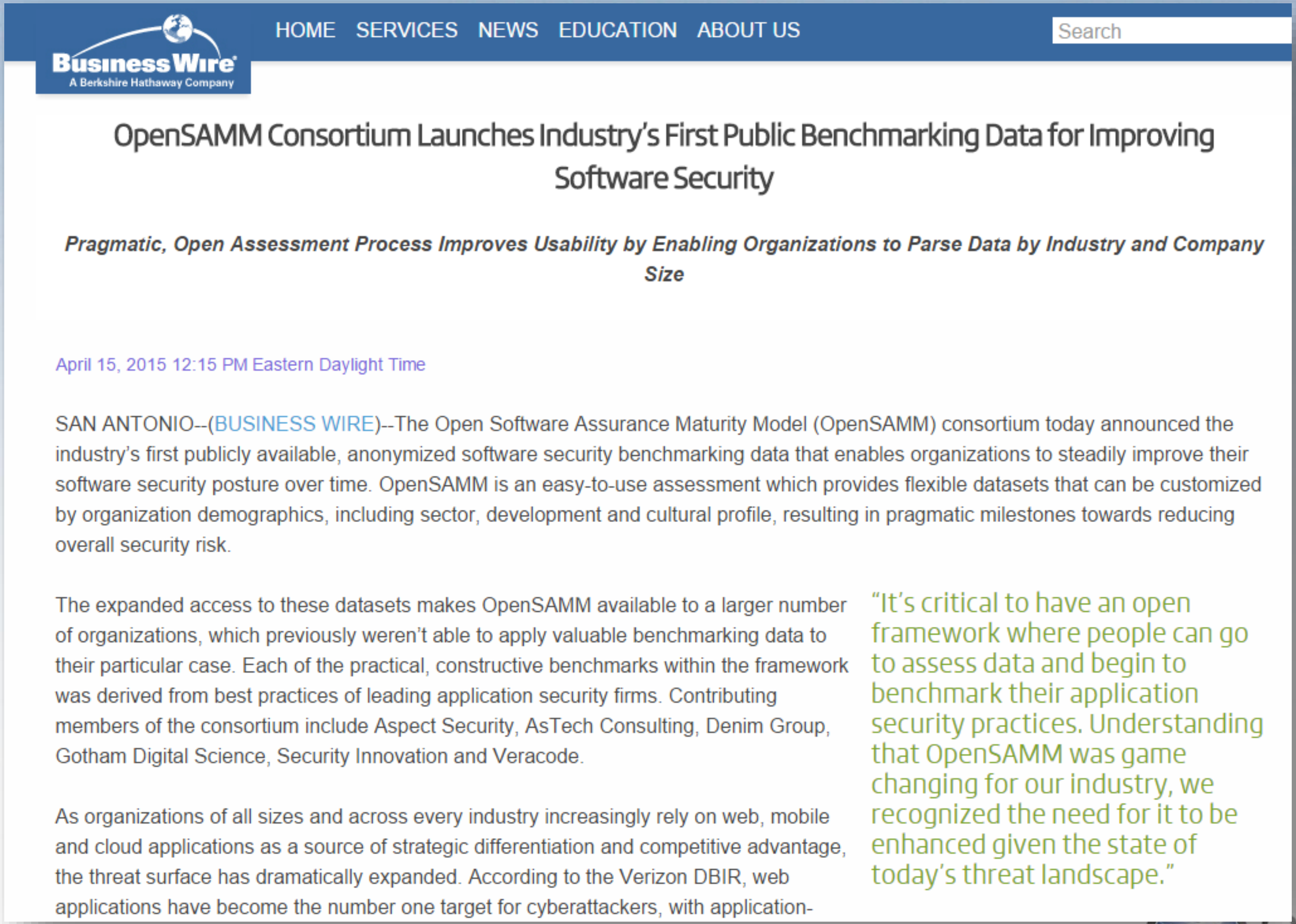
Evaluation Model
Questions, quality criteria, measurement model

Activity Model
Objectives, Activities, dependencies, metrics, ...

Supporting information / tools
Guidance, references, supporting tools, ...

Community feedback

How do I compare to?



HOME SERVICES NEWS EDUCATION ABOUT US
Search
Business Wire
A Berkshire Hathaway Company

OpenSAMM Consortium Launches Industry's First Public Benchmarking Data for Improving Software Security

Pragmatic, Open Assessment Process Improves Usability by Enabling Organizations to Parse Data by Industry and Company Size

April 15, 2015 12:15 PM Eastern Daylight Time

SAN ANTONIO--(BUSINESS WIRE)--The Open Software Assurance Maturity Model (OpenSAMM) consortium today announced the industry's first publicly available, anonymized software security benchmarking data that enables organizations to steadily improve their software security posture over time. OpenSAMM is an easy-to-use assessment which provides flexible datasets that can be customized by organization demographics, including sector, development and cultural profile, resulting in pragmatic milestones towards reducing overall security risk.

The expanded access to these datasets makes OpenSAMM available to a larger number of organizations, which previously weren't able to apply valuable benchmarking data to their particular case. Each of the practical, constructive benchmarks within the framework was derived from best practices of leading application security firms. Contributing members of the consortium include Aspect Security, AsTech Consulting, Denim Group, Gotham Digital Science, Security Innovation and Veracode.

> "It's critical to have an open framework where people can go to assess data and begin to benchmark their application security practices. Understanding that OpenSAMM was game changing for our industry, we recognized the need for it to be enhanced given the state of today's threat landscape."

As organizations of all sizes and across every industry increasingly rely on web, mobile and cloud applications as a source of strategic differentiation and competitive advantage, the threat surface has dramatically expanded. According to the Verizon DBIR, web applications have become the number one target for cyberattackers, with application-

Current roadmap

V2.0: end of 2019

2020:

- v2.1, 2.2, ...: iterative releases
- Agile/devops guidance
- Roadshows/trainings

Looking forward

- OWASP projects references
- Online assessments, integrated with benchmark data
- User community contributions
- Support for regulations
- SAMM user summits
- ...

Try it !

Questions? Feedback? Input?

#project-samm

github.com/OWASP/samm

SAMM newsletter

eepurl.com/gl9fb9

Credits

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

Sebastian Arriada - Argentina

Brett Crawley – United Kingdom

...

Thank You to Our Sponsors

MICRO FOCUS Fortify

CONCORD

nccgroup

splunk>

OWASP
Open Web Application
Security Project

OWASP
SAMM

SUPPORT OWASP SAMM

Software powers the world,
but insecure software threatens safety, trust,
and economic growth.

Call for sponsors

All proceeds from the sponsorship support the mission of the OWASP foundation and the further development of SAMM, funding

- marketing & PR support
- technical editing & UX support
- website development and hosting
- SAMM user summits
- core team summits
- tooling for the SAMM Benchmark project

info@owaspsamm.org

OWASP
Open Web Application
Security Project

Questions or Feedback ?

OWASP
Open Web Application
Security Project

Thank you

info@owaspsamm.org
seba@owasp.org