OWASP
Open Web Application
Security Project

OWASP SAMM v2.0

What is SAMM?

- The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.

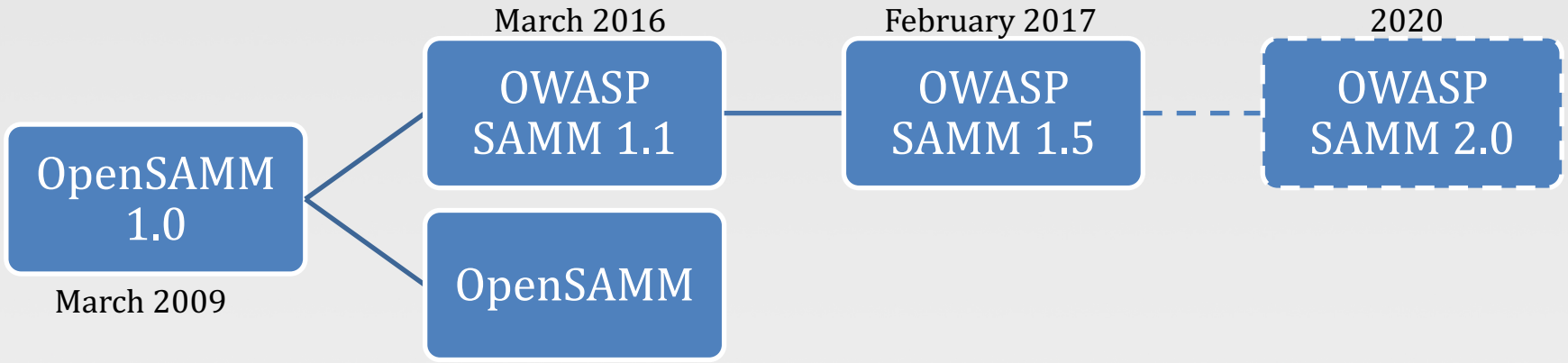
- The resources provided by SAMM will aid in:
  - *Evaluating an organization's existing software security practices.*
  - *Building a balanced software security assurance program in well-defined iterations.*
  - *Demonstrating concrete improvements to a security assurance program.*
  - *Defining and measuring security-related activities throughout an organization.*

Who is SAMM?

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

Sponsors:

Project History



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.”

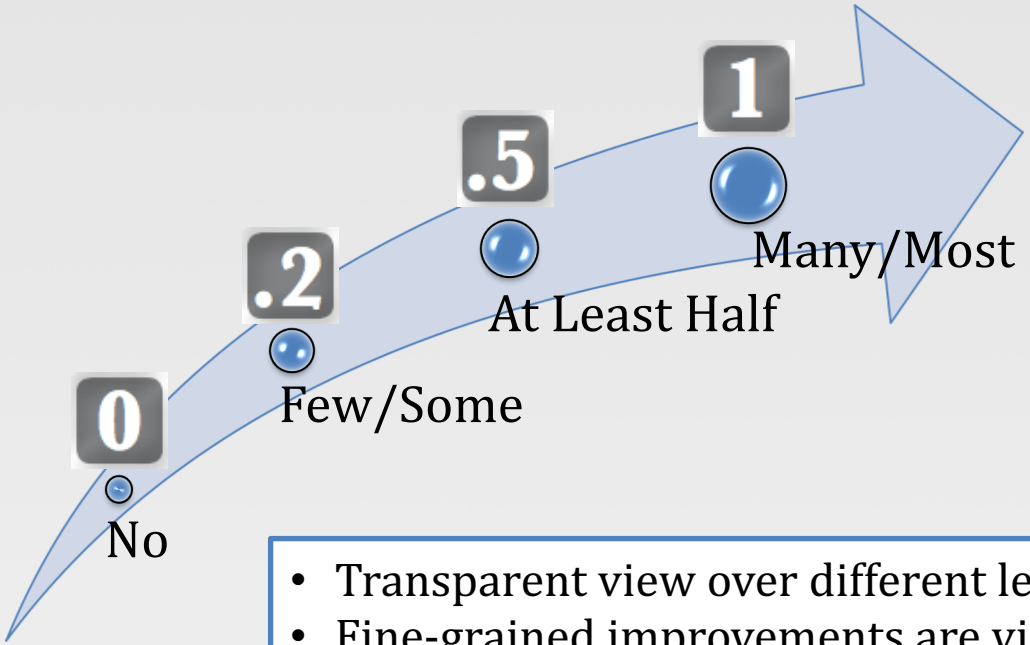
– George E. P. Box

Core Principles of SAMM

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)

Maturity Levels & Assessment Scores

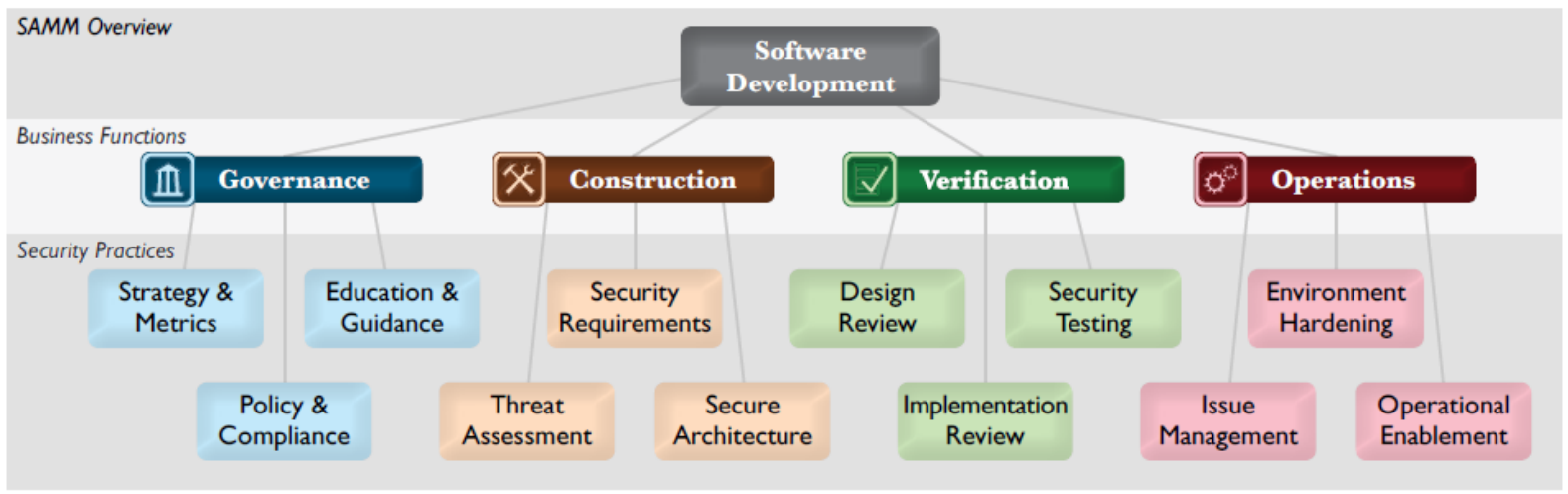
- **3** Comprehensive mastery at scale
- **2** Increased efficiency/effectiveness
- **1** Ad-hoc provision
- **0** Practice unfulfilled



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

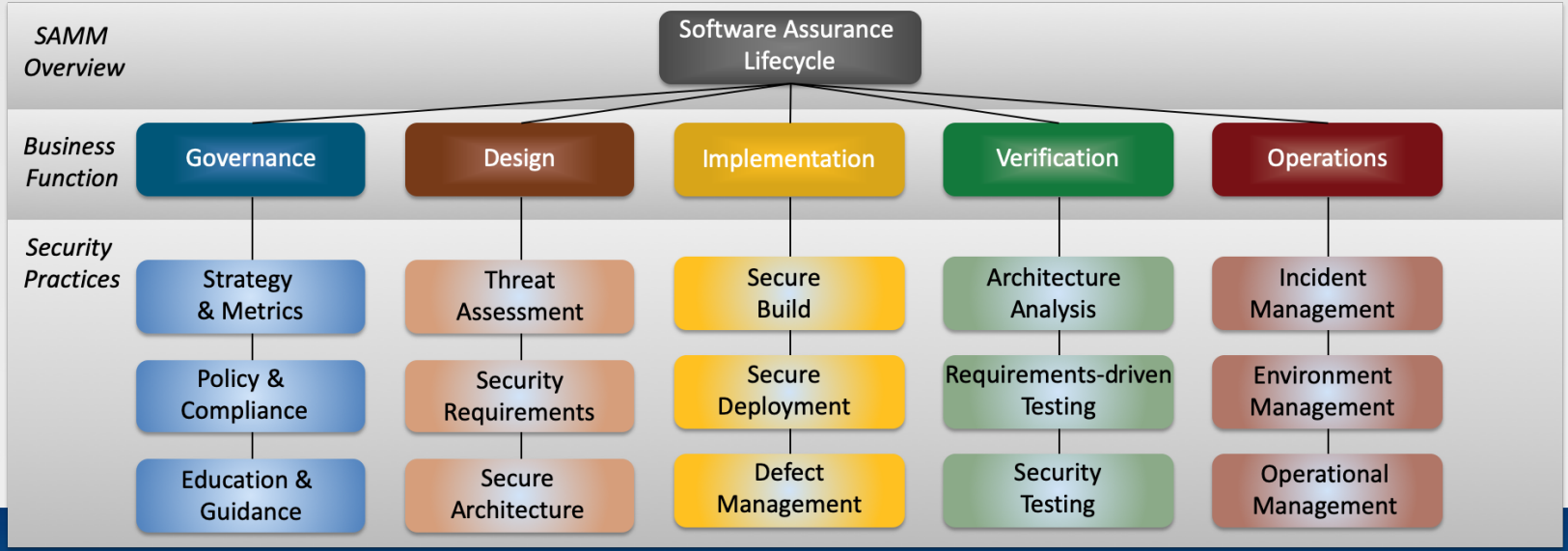
SAMM Framework v1.5

- For each of the four Business Functions, three Security Practices are defined
- The security practices cover areas relevant to software security assurance



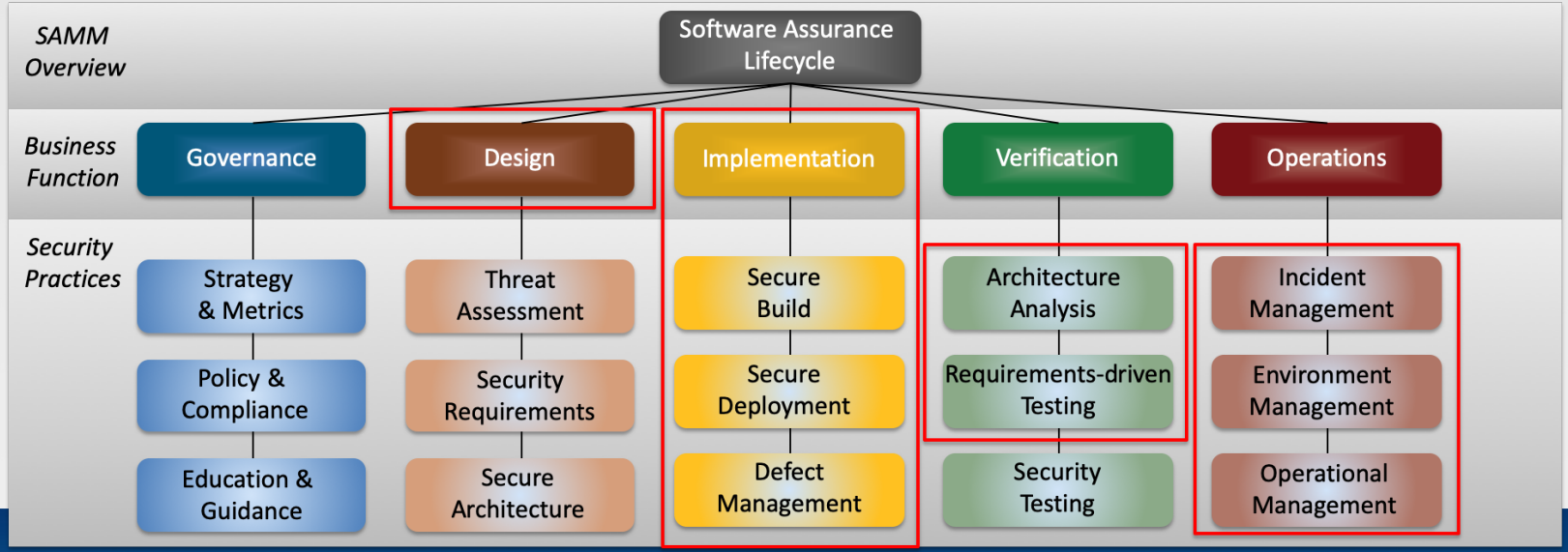
SAMM Framework v2.0

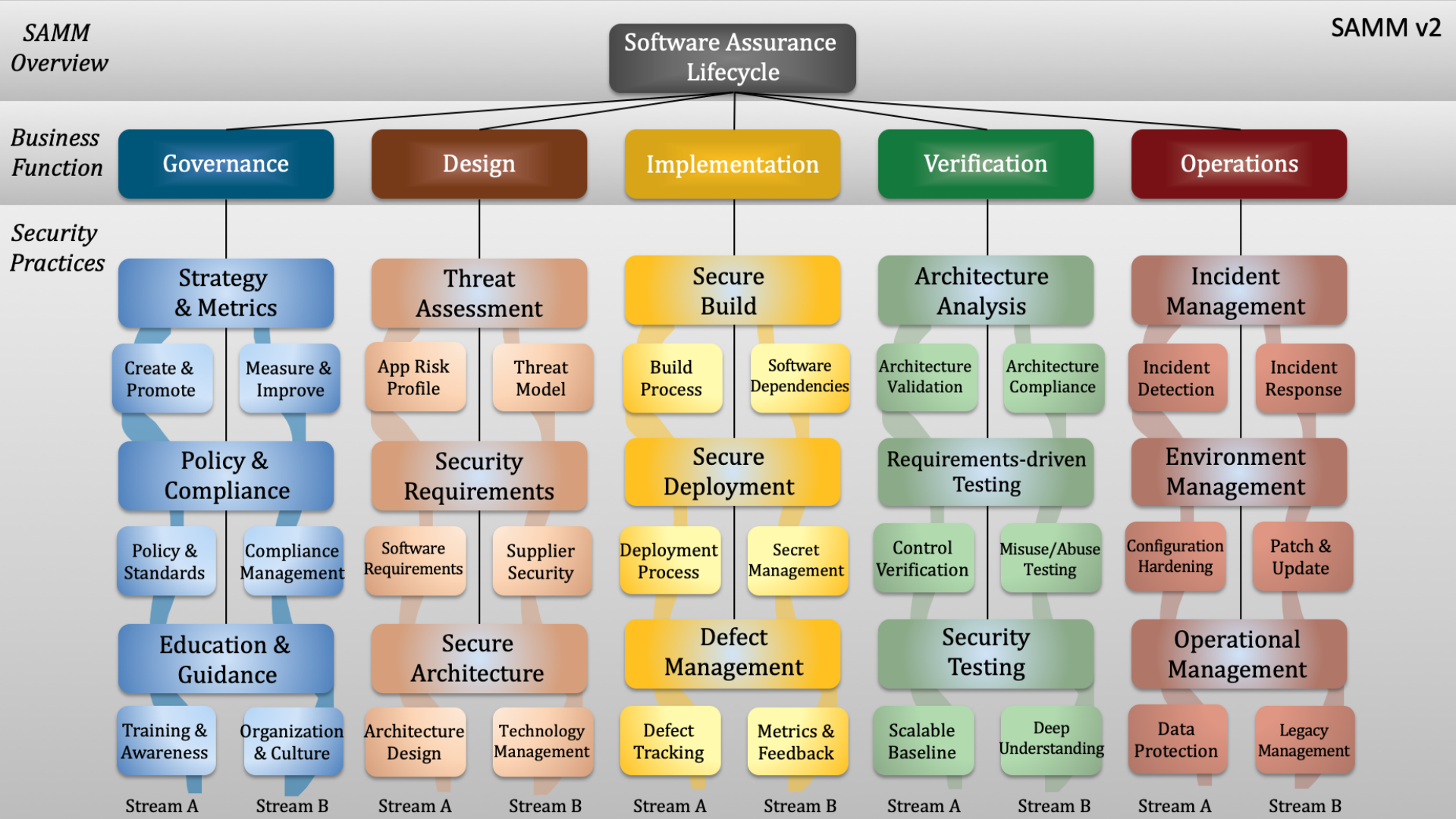
- For each of the five Business Functions, three Security Practices are defined
- The security practices cover areas relevant to software security assurance



SAMM Framework v2.0

- For each of the five Business Functions, three Security Practices are defined
- The security practices cover areas relevant to software security assurance




SAMM Overview
SAMM v2
Software Assurance Lifecycle
Business Function
Governance
Design
Implementation
Verification
Operations
Security Practices
Strategy & Metrics
Create & Promote
Measure & Improve
Policy & Compliance
Policy & Standards
Compliance Management
Education & Guidance
Training & Awareness
Organization & Culture
Threat Assessment
App Risk Profile
Threat Model
Security Requirements
Software Requirements
Supplier Security
Secure Architecture
Architecture Design
Technology Management
Secure Build
Build Process
Software Dependencies
Secure Deployment
Deployment Process
Secret Management
Defect Management
Defect Tracking
Metrics & Feedback
Architecture Analysis
Architecture Validation
Architecture Compliance
Requirements-driven Testing
Control Verification
Misuse/Abuse Testing
Security Testing
Scalable Baseline
Deep Understanding
Incident Management
Incident Detection
Incident Response
Environment Management
Configuration Hardening
Patch & Update
Operational Management
Data Protection
Legacy Management
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B

Assess via Toolbox

Governance			
Stream	**Level**	**Strategy & Metrics**	**Answer**
Create and Promote	**1**	**Do you prioritize applications based on a granular set of risks?**	
		You capture the risk appetite of your organization's executive leadership The organization's leadership vet and approve the set of risks You identify the main business and technical threats to your assets and data You document risks and store them in an accessible location	
	2	**Do you have a strategic plan for application security and use it to make decisions?**	
		The plan reflects the organization's business priorities and risk appetite The plan includes measurable milestones and a budget The plan is consistent with the organization's business drivers and risks The plan lays out a roadmap for strategic and tactical initiatives You have buy-in from 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, making sure they are available to all stakeholders	
Measure and Improve	**1**	**Do you use a set of metrics to measure the effectiveness and efficiency of the application security program across applications?**	
		You document each metric, including a description of the sources, measurement coverage, and guidance on how to use it to explain application security trends Metrics include measures of efforts, results, and the environment measurement categories Most of the metrics are frequently measured, easy or inexpensive to gather, and expressed as a cardinal number or a percentage Application security and development teams publish metrics	
	2	**Did you define Key Perfomance Indicators (KPI) from available application security metrics?**	
		You defined KPIs after gathering enough information to establish realistic objectives You developed KPIs with the buy-in from the leadership and teams responsible for application security KPIs are available to the application teams and include acceptability thresholds and guidance in case teams need to take action Success of the application security program is clearly visible based on defined KPIs	
	3	**Do you update the Application Security strategy and roadmap based on application security metrics and KPIs?**	
		You review KPIs at least yearly for their efficiency and effectiveness KPIs and application security metrics trigger most of the changes to the application security strategy	

Dashboards

Current Maturity Score

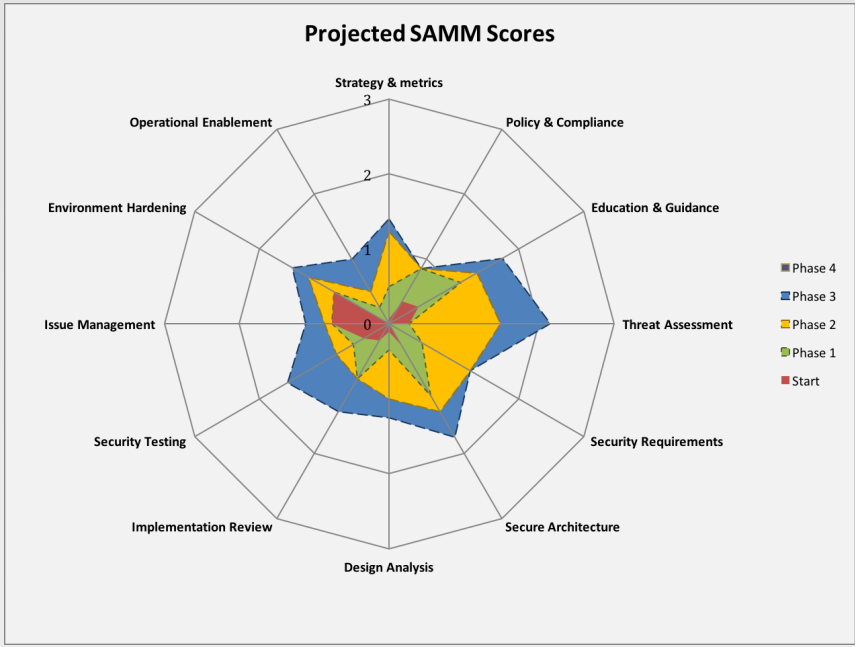
Functions	Security Practices	Current	Maturity 1	Maturity 2	Maturity 3
Governance	Strategy & Metrics	0.63	0.25	0.13	0.25
Governance	Policy & Compliance	1.00	0.25	0.13	0.63
Governance	Education & Guidance	0.75	0.13	0.00	0.63
Design	Threat Assessment	1.25	0.25	0.25	0.75
Design	Security Requirements	0.88	0.50	0.25	0.13
Design	Secure Architecture	1.75	0.50	0.25	1.00
Implementation	Secure Build	0.75	0.25	0.25	0.25
Implementation	Secure Deployment	1.13	0.38	0.38	0.38
Implementation	Defect Management	0.63	0.25	0.25	0.13
Verification	Architecture Assessment	0.88	0.38	0.25	0.25
Verification	Requirements Testing	1.25	0.75	0.38	0.13
Verification	Security Testing	1.63	0.75	0.38	0.50
Operations	Incident Management	1.63	0.38	0.63	0.63
Operations	Environment Management	0.75	0.25	0.50	0.00
Operations	Operational Management	0.88	0.50	0.25	0.13

Functions	Current
Governance	0.79
Design	1.29
Implementation	0.83
Verification	1.25
Operations	1.08

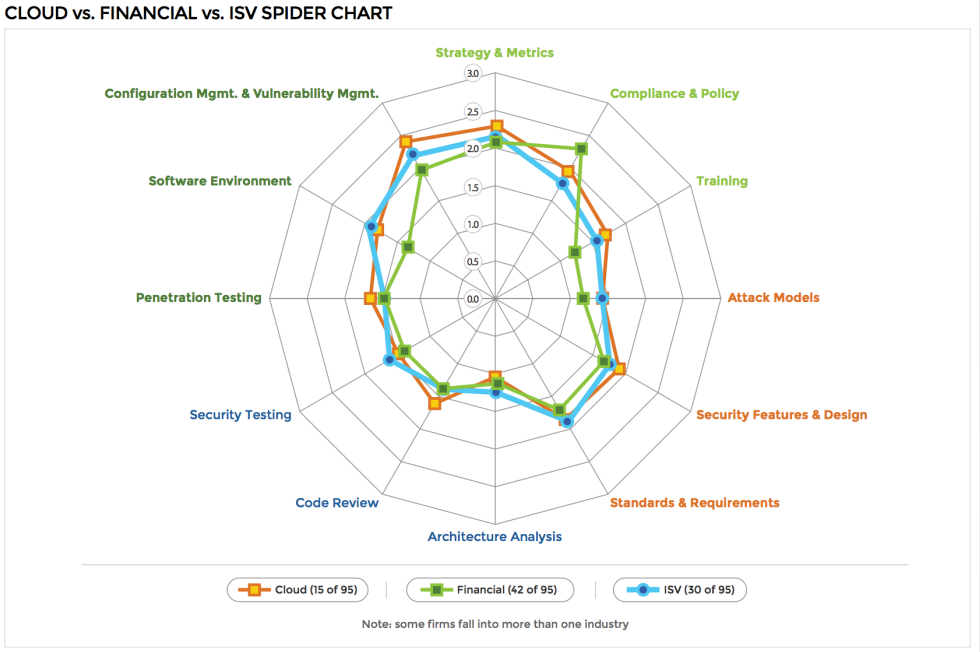
Critical Success Factors

- Get buy-in from stakeholders
- Adopt a risk-based approach
- Awareness & Education is the foundation
- Integrate & automate security in your development, acquisition, and deployment processes
- Measure: Provide Management Visibility

SAMM can(sorta) map to BSIMM



SAMM



BSIMM

SAMM BENCHMARK

Time to answer the question…

How do I compare?

https://owaspsamm.org/benchmarking/

What is SAMM Benchmark

- 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 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.

Data Contributions

Verified Data Contribution

- Scenario 1: The submitter is known and has agreed to be identified as a contributing party.
- Scenario 2: The submitter is known but would rather not be publicly identified.
- Scenario 3: The submitter is known but does not want it recorded in the dataset.

Unverified Data Contribution

- Scenario 4: The submitter is anonymous.

Contribution Process

There are a few ways that data can be contributed:

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

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

Data Structure

The following data elements are required* or optional:

- *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)

Get involved

- Website: https://owaspsamm.org
- Github: https://github.com/OWASP/samm/
- Slack: OWASP - #project-samm
- Use and donate (feed)back!
- Donate resources
- Sponsor SAMM

SAMM Newsletter

Thank you!

Questions?

brian.glas@owasp.org (or @gmail.com)
@infosecdad