OWASP
Open Web Application
Security Project

OWASP
SAMM

Bootstrap and Improve Your SDLC with OWASP SAMM - ASAP!

Event Name

Event Date

OWASP
Open Web Application
Security Project

OWASP
Open Web Application Security Project

How About You?

A little bit about you!

- What is your SAMM experience?
- Your role in application security?
- Specific areas you'd like to cover?

This Training Will Cover:

- SAMM 2.0
- How to apply OWASP SAMM in practice
- Looking into different practices from a practical perspective
- Discuss some of the challenges that you might face
- Open interaction session

Day 1 Schedule

Part One

SDLC Overview & OWASP SAMM Introduction

- The Application Security Challenge
- Software Development Lifecycle (SDLC) Overview
- OWASP SAMM - Vision, History, Structure
- OWASP SAMM As an Assessment Tool

Part Two

OWASP SAMM Tools

- Tools of the Trade
- SAMM Assessment Toolkit
- Benchmark Project
- Leveraging OWASP Projects and Tools

Day 2 Schedule

Part Three

Applying OWASP SAMM

- Methodology
- Establishing Assessment Scope
- Assessing Governance
- Assessing Design
- Assessing Implementation
- Assessing Verification
- Assessing Operations
- Setting Maturity Targets & Improvement Activities

Part Four

OWASP SAMM Best Practices

- Choosing the Right Starting Points
- Metrics and Management
- Achieving Security by Design
- Critical Success Factors

Preparation

Download the OWASP SAMM Toolbox:

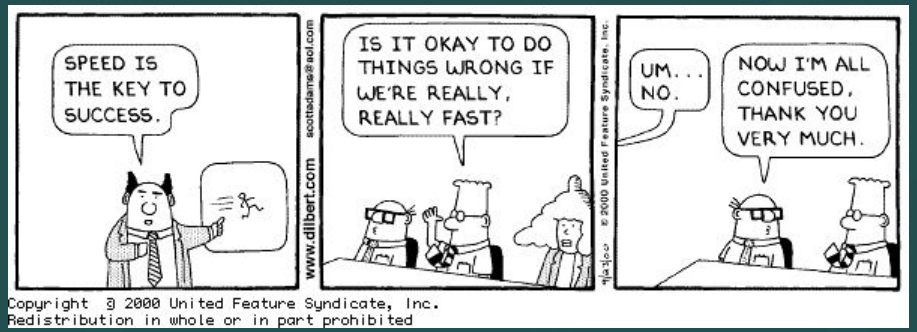
https://github.com/OWASP/samm/tree/master/Supporting%20Resources/v2.0/toolbox/

Part One

SDLC Overview & OWASP SAMM Introduction

- *The Application Security ~~Challenge~~ Opportunity*
- Software Development Lifecycle (SDLC) Overview
- OWASP SAMM - Vision, History, Structure
- OWASP SAMM As an Assessment Tool

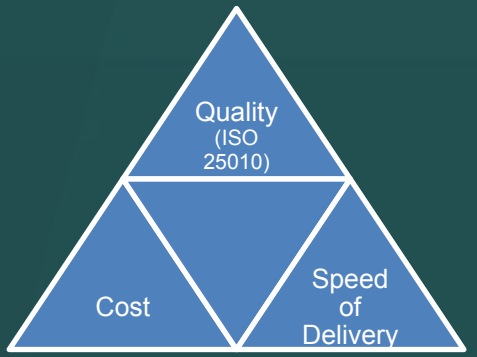
Application Security Problem



Compliance Availability

Technology Risk Integrity

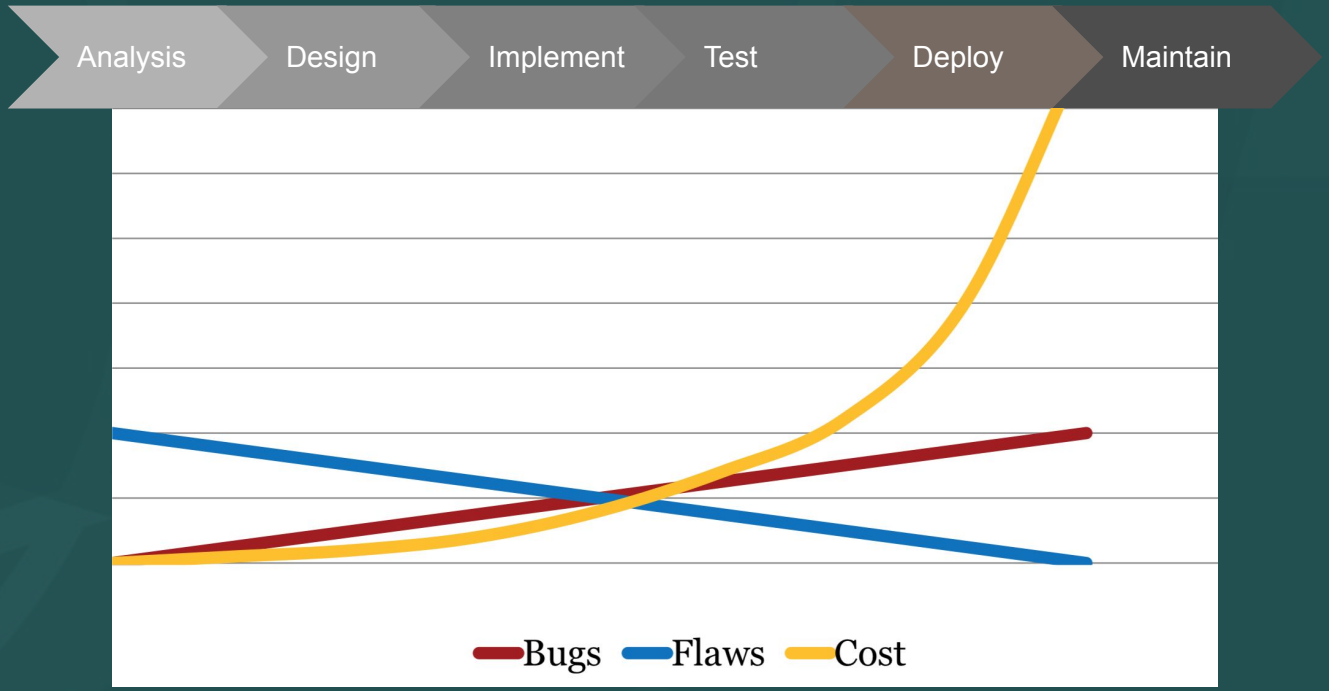
Confidentiality Cloud Microservices



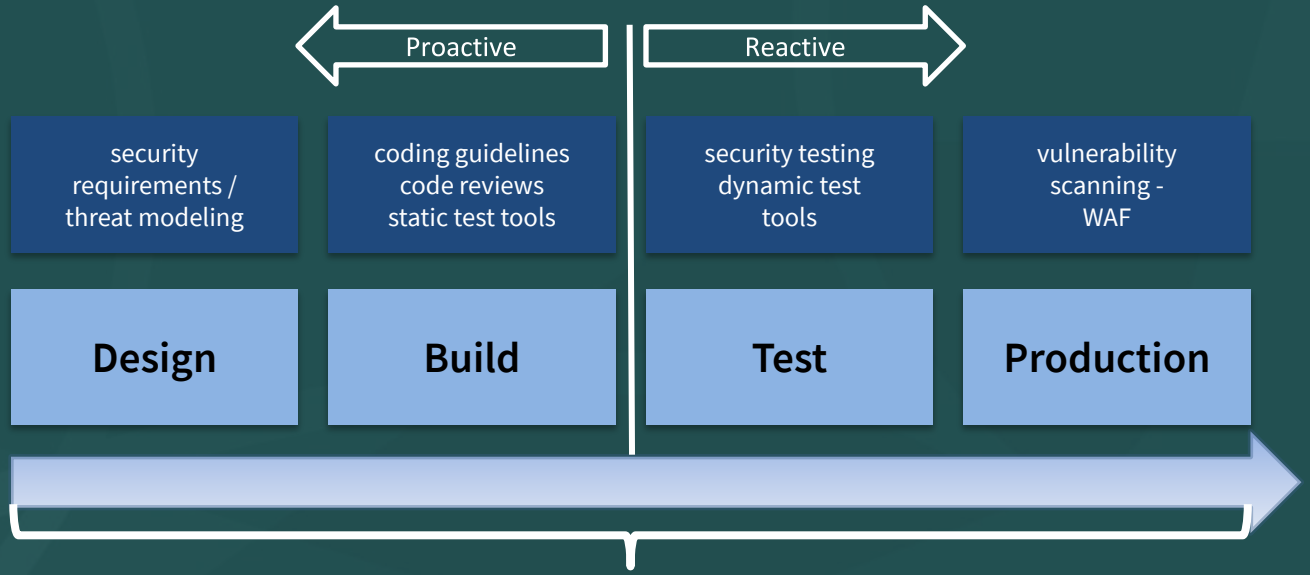
79% of vulnerabilities are application related

OWASP
Open Web Application
Security Project

Application Security Costs



“Build in” Software Assurance



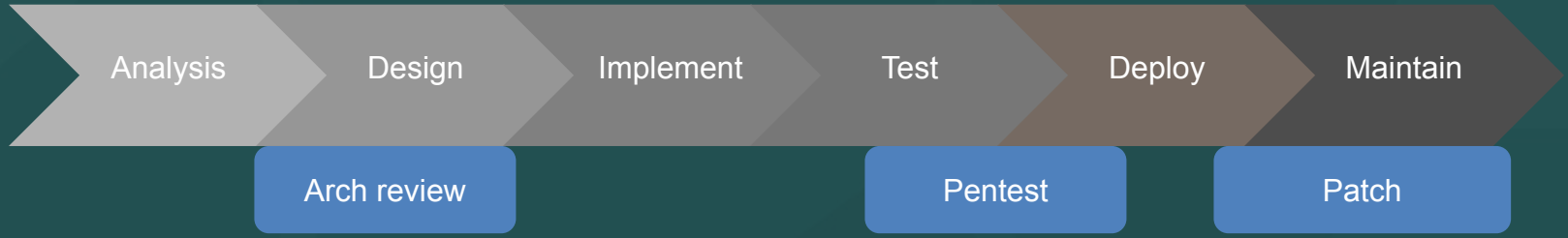
Secure Development Life Cycle

Part One

SDLC Overview & OWASP SAMM Introduction

- The Application Security Opportunity
- *Software Development Lifecycle (SDLC) Overview*
- OWASP SAMM - Vision, History, Structure
- OWASP SAMM As an Assessment Tool

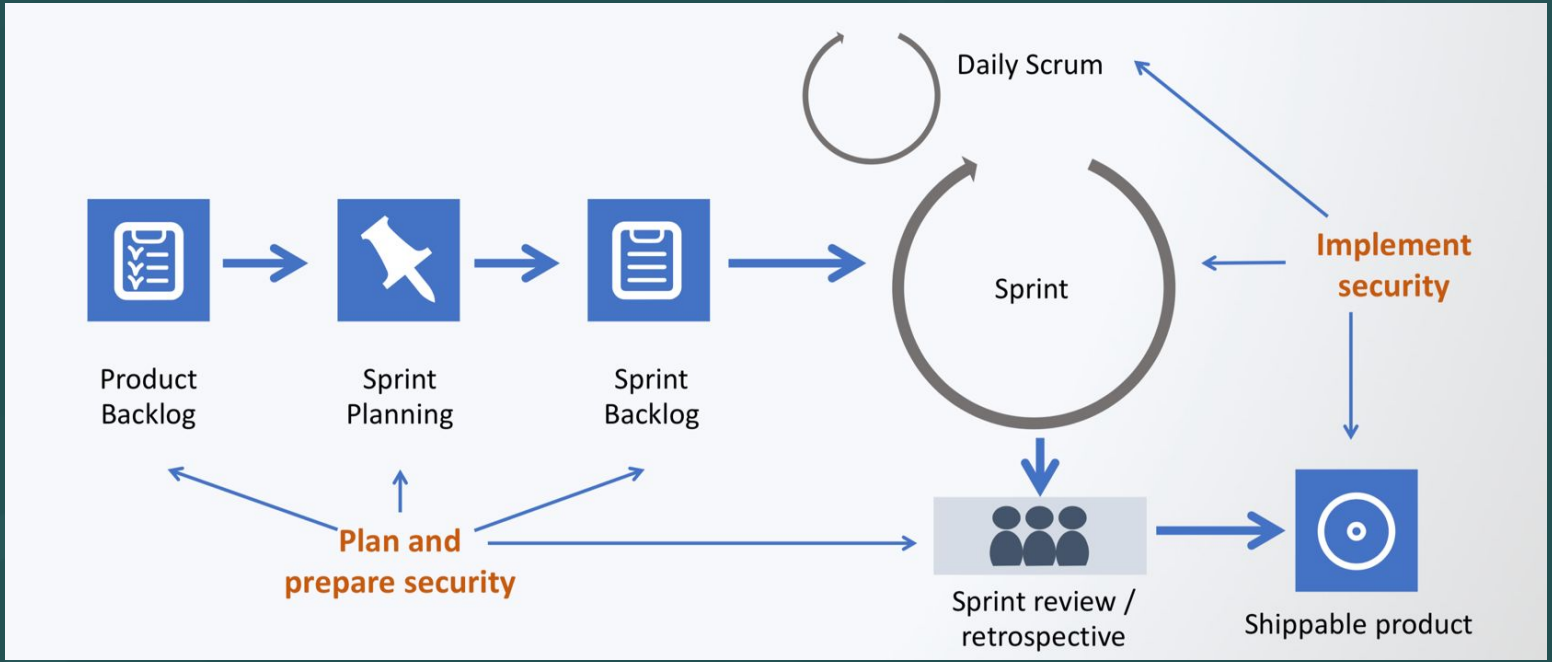
Typical SDLC



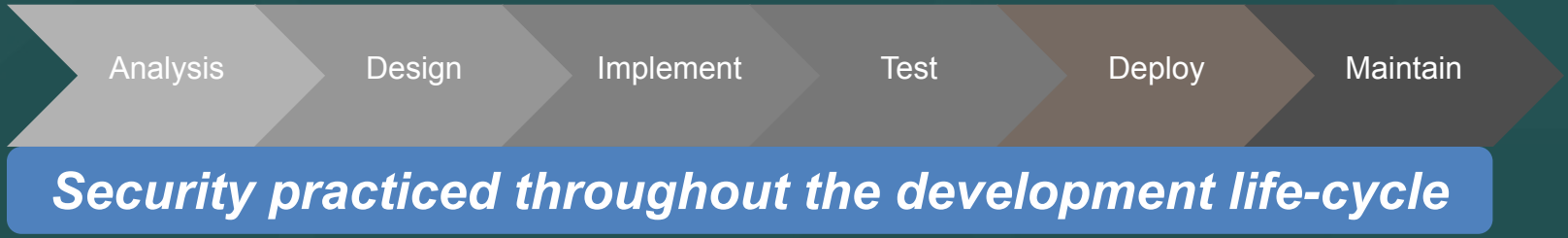
Problematic, since:

- Focus on bugs, not flaws
- Not cost efficient
- No security assurance
  - All bugs found ?
  - Bug-fix fixes all occurrences ? (also future ?)
  - Bug-fix might introduce new security vulnerabilities

Security In Agile Scrum



Secure by Design



Enterprise-wide software security improvement program

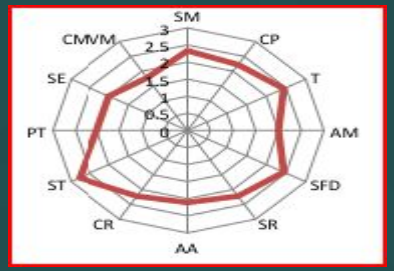
- Strategic approach to assure software quality
- Goal is to increase systematicity
- Focus on security functionality and security hygiene

SDLC Cornerstones

SDLC Initiatives

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

NIST
National Institute of Standards and Technology



SSE CMM

Software Engineering Institute | Carnegie Mellon

Software Assurance Maturity Model
A guide to building security into software development
Version - 1.0

OWASP
Open Web Application Security Project

Part One

SDLC Overview & OWASP SAMM Introduction

- The Application Security Opportunity
- Software Development Lifecycle (SDLC) Overview
- *OWASP SAMM - Vision, History, Structure*
- OWASP SAMM As an Assessment Tool

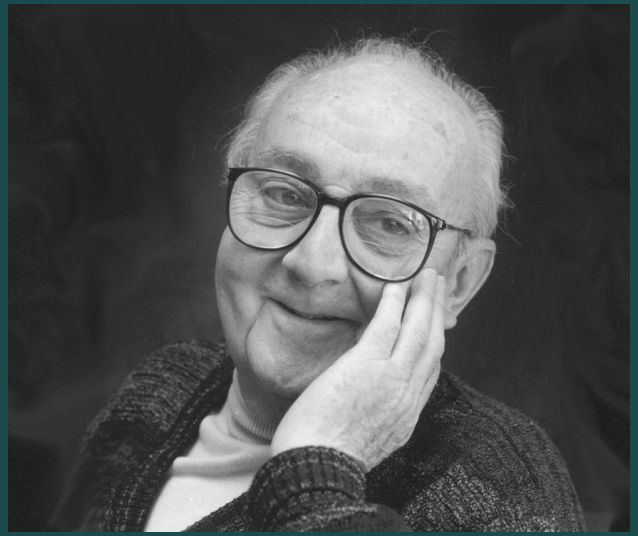
SAMM principles

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)

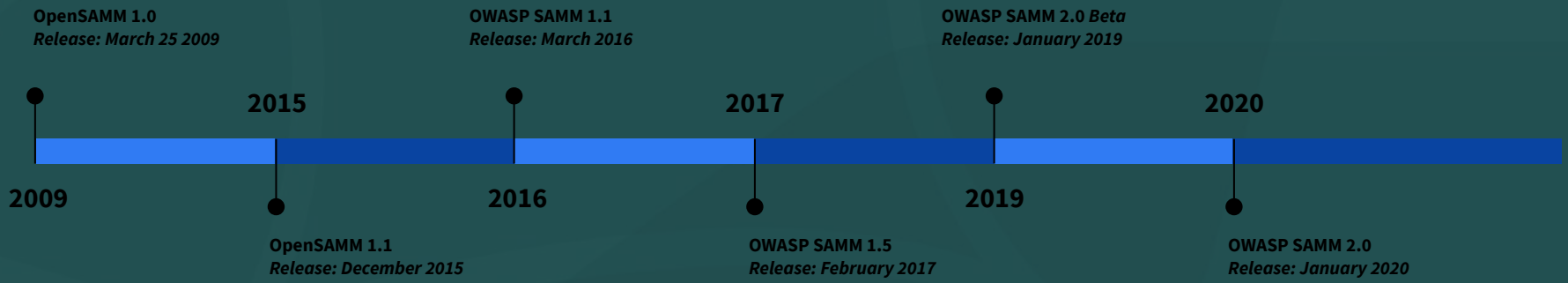
Why SAMM?

"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



Project History



OWASP
Open Web Application Security Project

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

FLAGSHIP mature projects

OWASP
Open Web Application Security Project

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

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

Who is SAMM today?

- Sebastien (Seba) Deleersnyder
  - *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
- Bart De Win
  - *Project Co-Leader, Belgium*
- Patricia Duarte – Uruguay
- John Kennedy – Sweden
- Hardik Parekh - United States
- John Ellingsworth - United States
- Sebastian Arriada - Argentina
- Brett Crawley – United Kingdom

Sponsors:

CONCORD

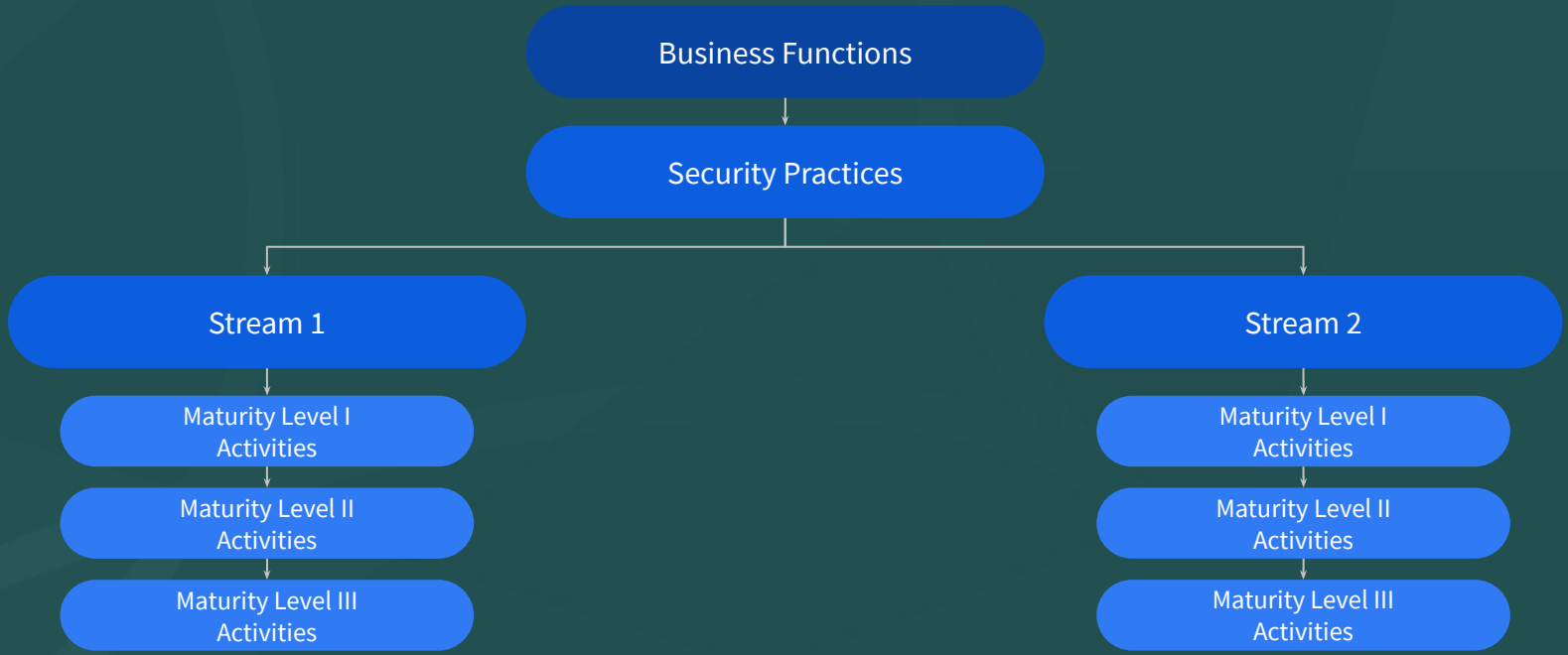
MICRO FOCUS Fortify

nccgroup

splunk>

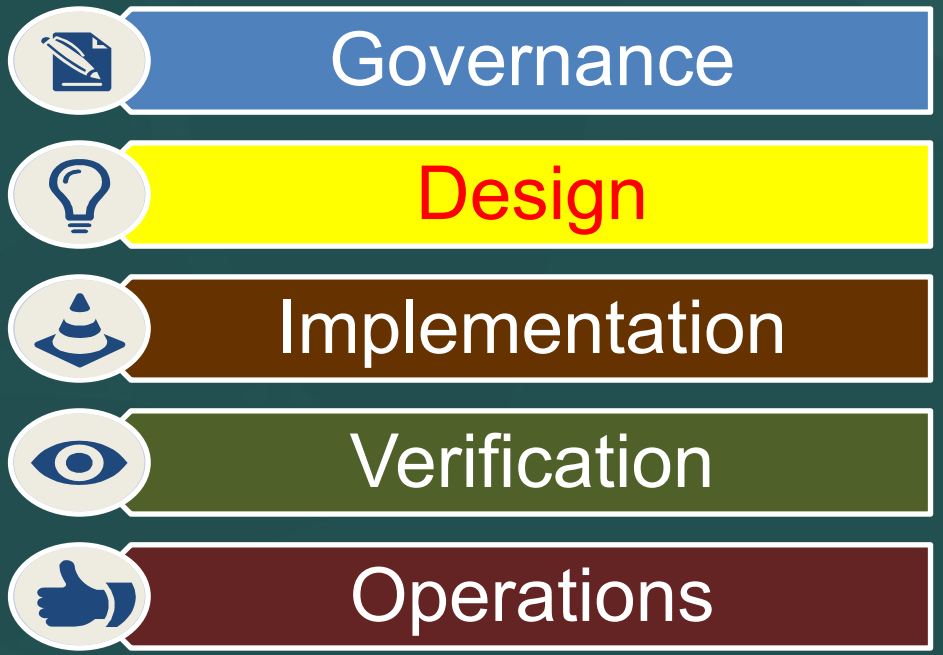
OWASP
Open Web Application Security Project

OWASP SAMM Structure



SAMM Business Functions

- Start with the core activities tied to any organization performing software development
- Named generically, but should resonate with any development stakeholder



SAMM Security Practices

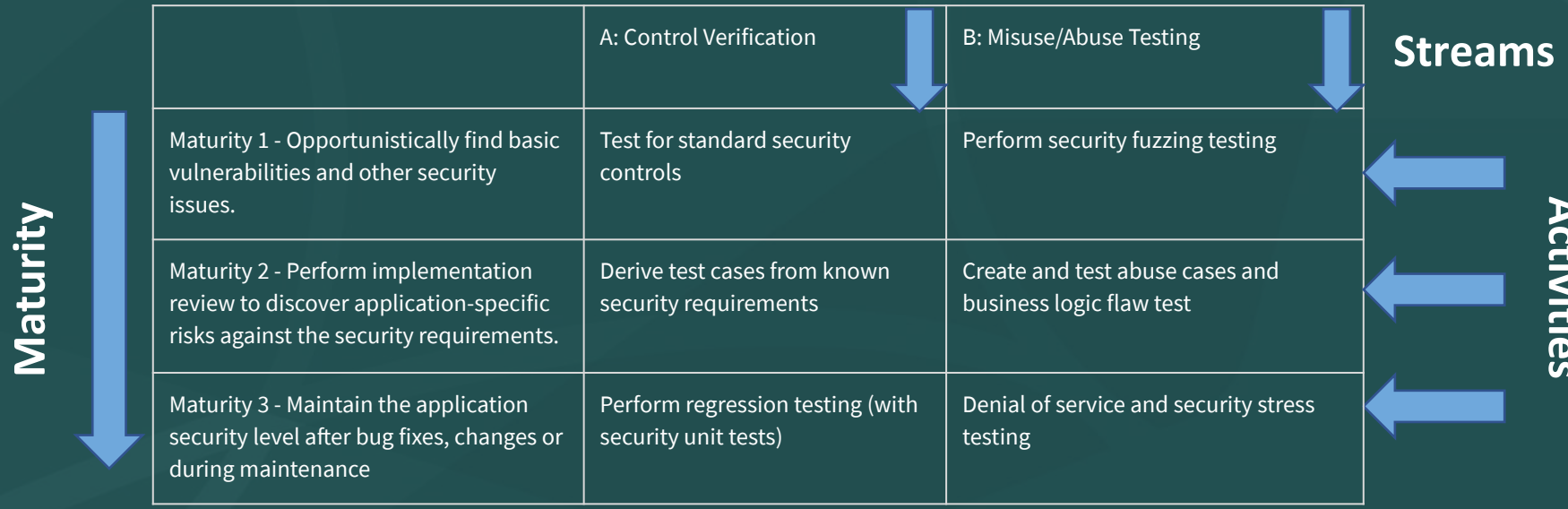
- From each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one an ‘silo’ for improvement

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

Under Each Security Practice

- Three successive Objectives under each Practice define how it can be improved over time
  - This establishes a notion of a Level at which an organization fulfills a given Practice
- The three Levels for a Practice generally correspond to:
  - (0: Implicit starting point with the Practice unfulfilled)
  - 1: Initial understanding and ad hoc provision of the Practice
  - 2: Increase efficiency and/or effectiveness of the Practice
  - 3: Comprehensive mastery of the Practice at scale

Activity Streams & Maturity Level



	A: Control Verification	B: Misuse/Abuse Testing
Maturity 1 - Opportunistically find basic vulnerabilities and other security issues.	Test for standard security controls	Perform security fuzzing testing
Maturity 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
Maturity 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

This security practice focuses on creating and integrating both positive (Control Verification) and negative (Misuse/Abuse Testing) security tests based on requirements (user stories).

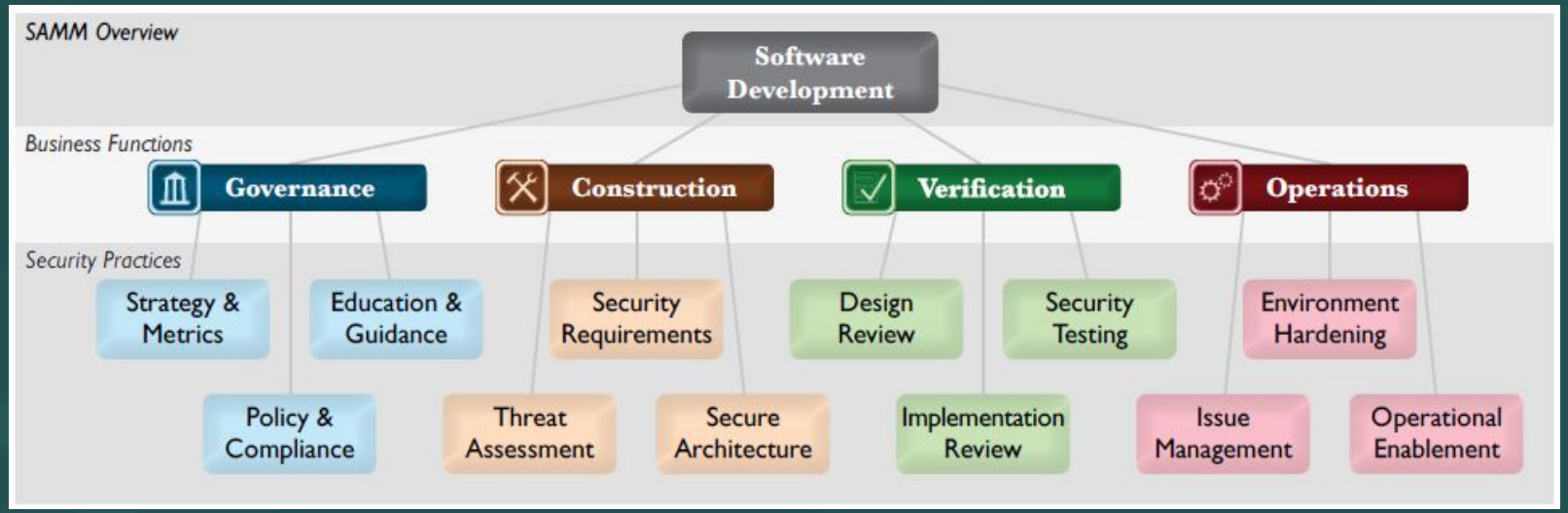
Maturity levels and scoring

- 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 Core Framework v1.5

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



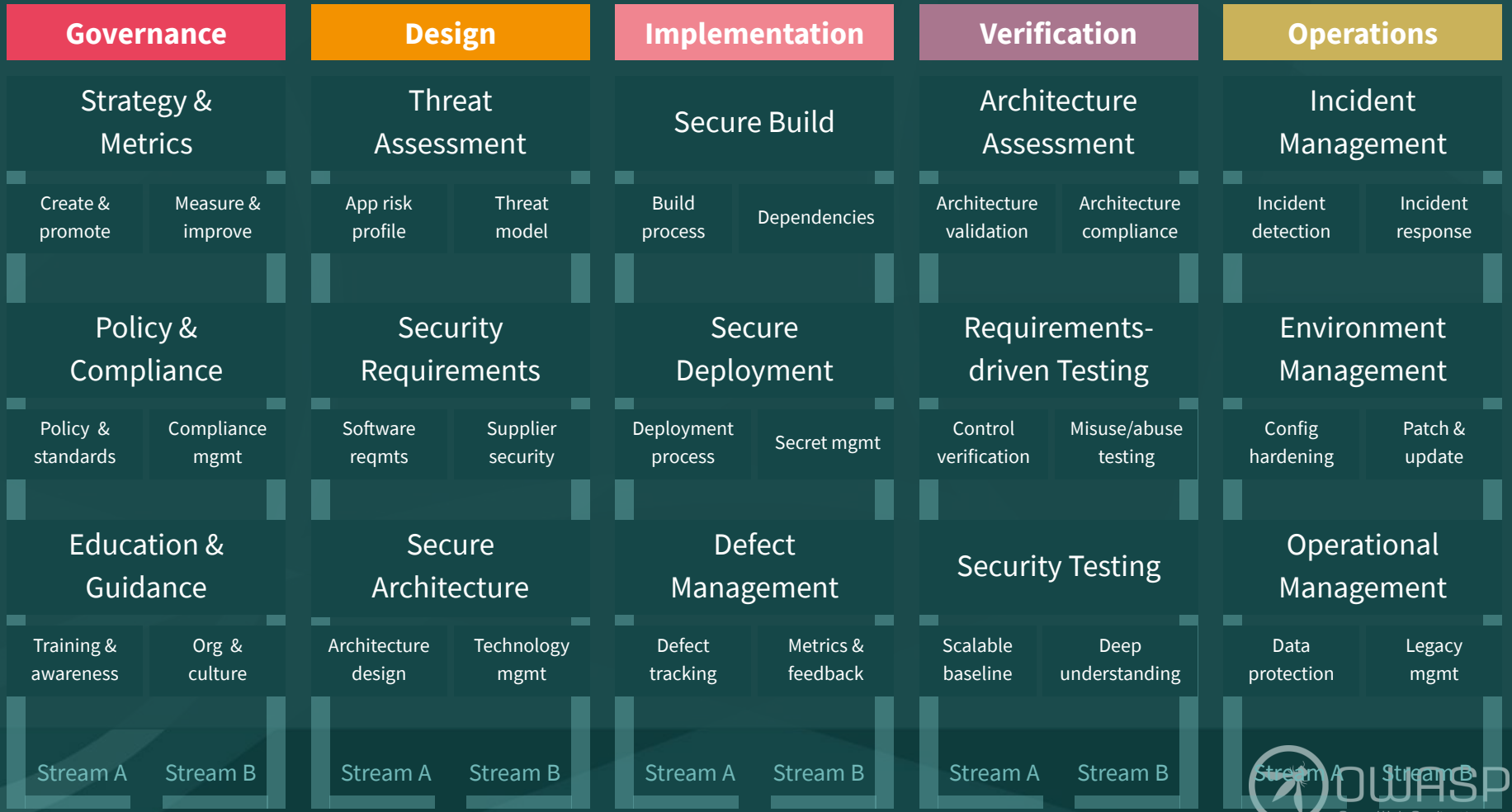
SAMM Core Framework v2.0

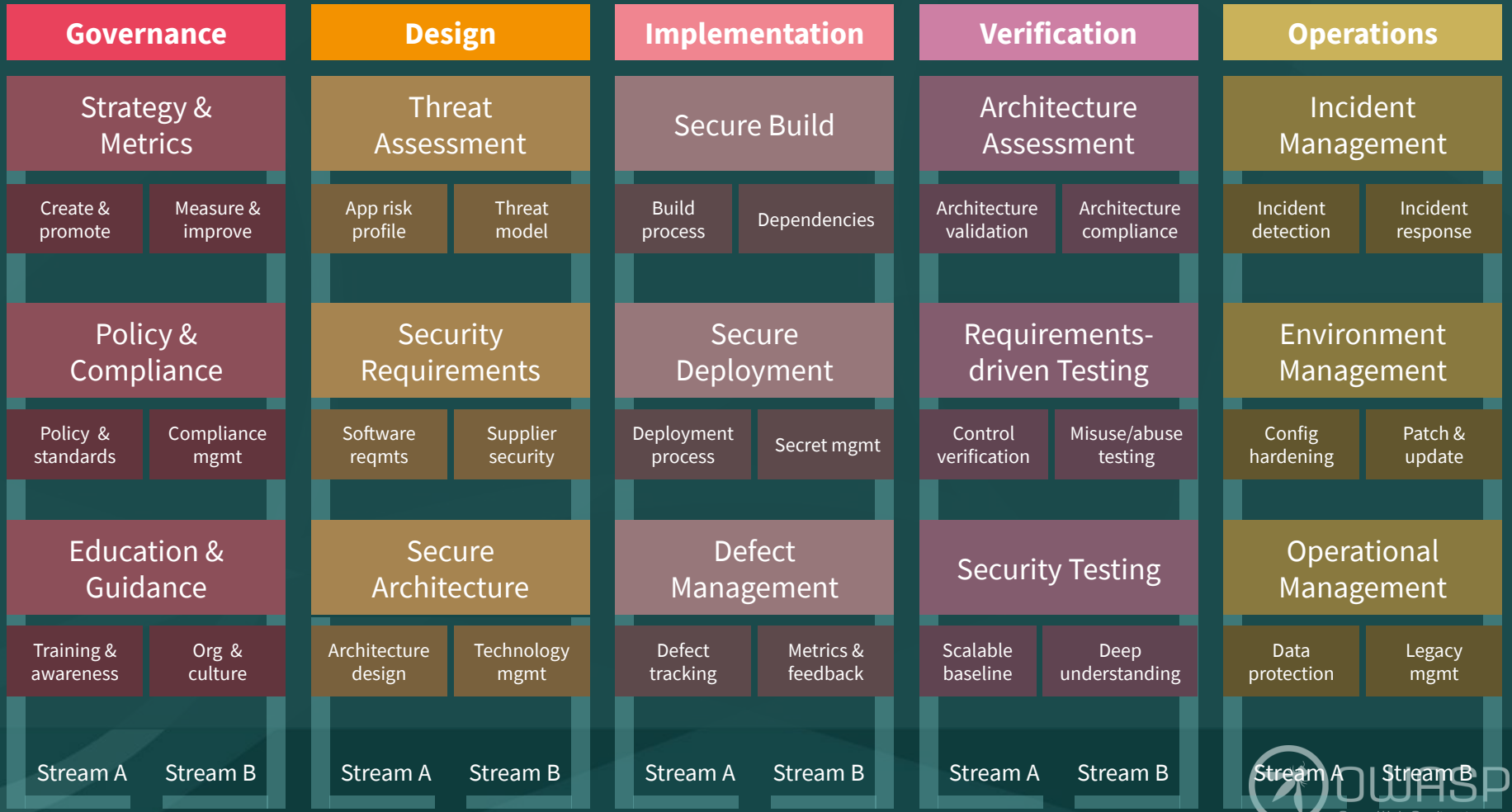
Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education & Guidance	Secure Architecture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

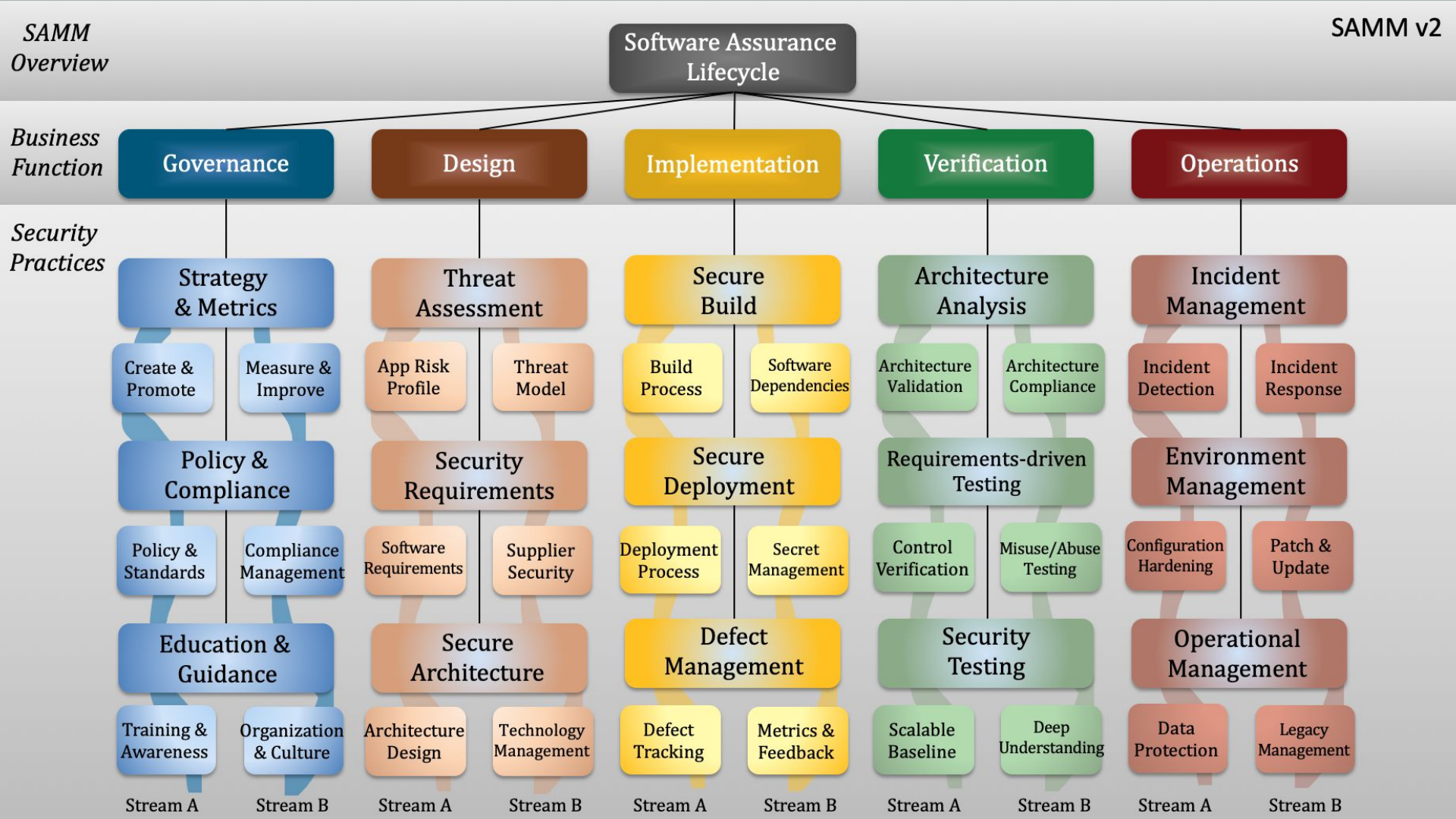
SAMM Core Framework v2.0

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




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

Key Changes in SAMM v2.0

SAMM v1.5

Four Business Functions - Governance, Construction, Verification, Operations

- 12 Security Practices

Very little, if any, prescriptive guidance for build and deploy domains

Maturity level activities could be orphaned, and sometimes unrelated to each other

Maturity level activities not in order of increasing difficulty, cost of implementation

Coverage based measurement

SAMM v2.0

Five Business Functions - Governance, Design, Implementation, Verification, Operations

- 15 Security Practices

New Business Function "Implementation" to accommodate guidance related to build and deploy domains

Maturity level activities are aligned and linked per *Stream*. Each stream has a clear *Objective*

Maturity level activities designed in order of increasing difficulty, implementation cost

Coverage & Quality based measurement

Part One

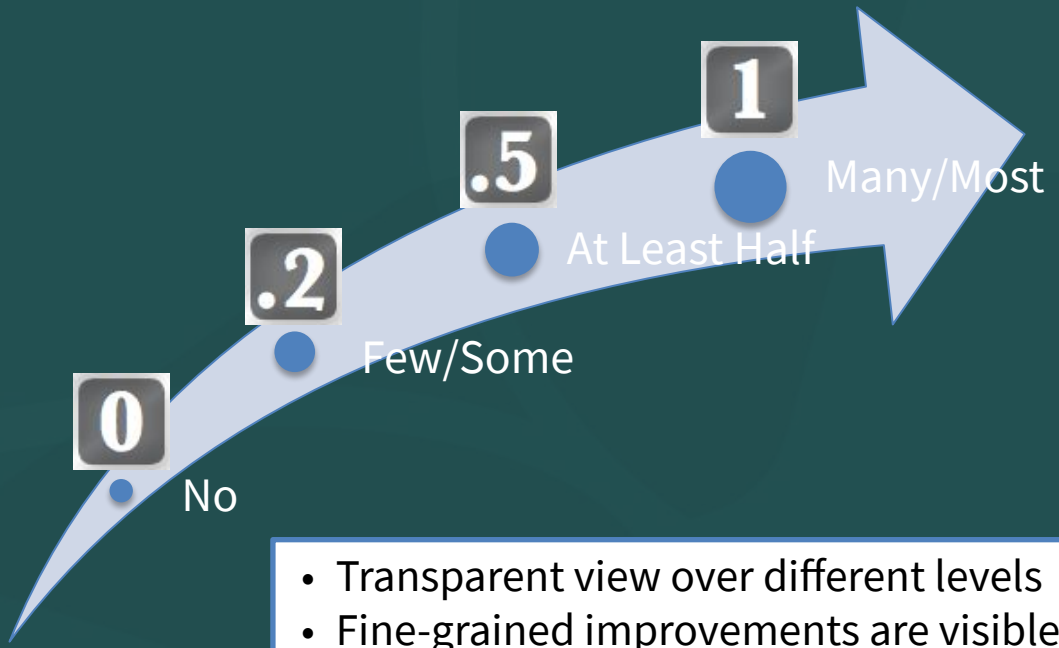
SDLC Overview & OWASP SAMM Introduction

- The ‘Application Security Problem’
- Software Development Lifecycle (SDLC) Overview
- OWASP SAMM - Vision, History, Structure
- *OWASP SAMM As an Assessment Tool*

Applying the Assessment

Maturity Assessment Levels

- **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

Assessment Process

Assess activities along two axes:

- **Coverage**, by means of *questions*
- **Quality**, by means of mandatory *criteria*

Business Functions	Current
Governance	1.92
Design	1.46
Implementation	1.92
Verification	1.79
Operations	1.04

Stream	Level	Requirements Testing	Answer			Rating
A: Control Verification	1	**Do you test applications for the correct functioning of standard security controls?**	**Yes, the majority of them**	1	0.750	**0.95**
		QC: Security testing at least verifies the implementation of authentication, access control, input validation, encoding and escaping data, and encryption controls.				
		QC: Security testing executes whenever the application changes its use of the controls.				
	2	**Do you test security controls based on the specific application security requirements?**	**Yes, some of them**	0.2	0.200	
		QC: Tests are tailored to each application and assert expected security functionality.				
		QC: Test results are captured as a pass or fail condition				
	3	**Do you automatically test applications for security regressions?**	**No**	0	0.000	
		QC: Tests are consistently written for all identified bugs (possibly exceeding a pre-defined severity threshhold)				
		QC: Security tests are collected in a test suite that is part of the existing unit testing framework				
B: Misuse/Abuse Testing	1	**Do you test applications using randomization techniques?**	**Yes, at least half of them**	0.5		
		QC: Testing covers most or all of the application's main input parameters				
		QC: All application crashes are recorded and systematically inspected for security impact				
	2	**Do you create abuse cases from functional requirements and use them to drive security tests?**	**Yes, sometimes**	0.2		
		QC: Important business functionality has corresponding abuse cases				
		QC: You build abuse stories around relevant personas with well-defined motivations and characteristics				
		QC: You capture identified weaknesses as security requirements				
	3	**Do you perform denial of service and security stress testing?**	**No**	0		
		QC: Stress tests target specific application resources (e.g. memory exhaustion by saving large amounts of data to a user session)				
		QC: You design tests around relevant personas with well-defined capabilities (knowledge, resources)				

Maturity Score = Sum(Avg(StreamALevel1,StreamBLevel1)+Avg(StreamALevel2,StreamBLevel2)+Avg(StreamALevel3,StreamBLevel3))

Creating Scorecards

Gap analysis

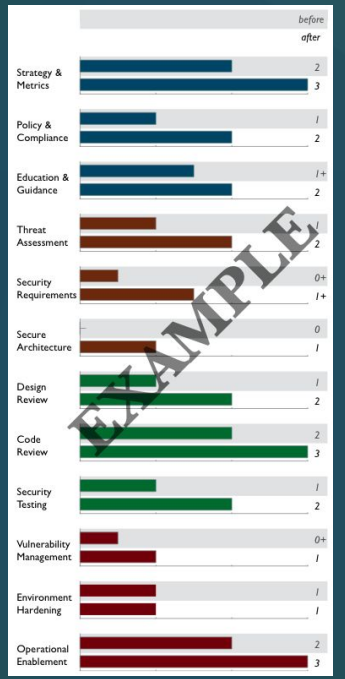
- Capturing scores from detailed assessments versus expected performance levels

Demonstrating improvement

- Capturing scores from before and after an iteration of assurance program build-out

Ongoing measurement

- Capturing scores over consistent timeframe for an assurance program already in place



OWASP
Open Web Application Security Project

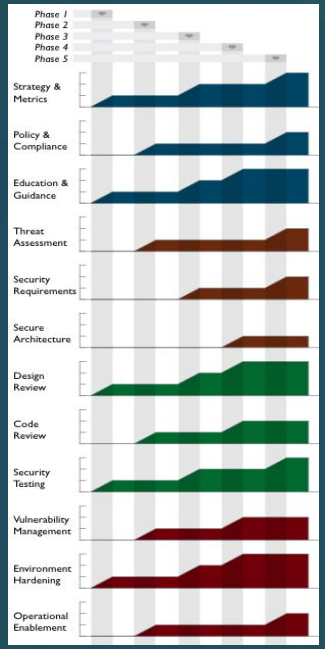
Roadmap Templates

To make the “building blocks” usable, SAMM defines Roadmap templates for typical kinds of organizations

- Independent Software Vendors
- Online Service Providers
- Financial Services Organizations
- Government Organizations

Organization types chosen because

- They represent common use-cases
- Each organization has variations in typical software-induced risk
- Optimal creation of an assurance program is unique



Part Two

OWASP SAMM Tools

- *Tools of the Trade*
- SAMM Assessment Toolkit
- Benchmark Project
- Leveraging OWASP Projects & Tools

OWASP SAMM Tools

- Translations (Spanish, Japanese, *German,* Ukrainian, …)
- Assessment questionnaire(s)
- Roadmap chart template
- Project plan template
- OWASP SAMM-BSIMM mapping
- Benchmark Project
- Mappings to security standards
  - ISO/IEC 27034, PCI, etc.

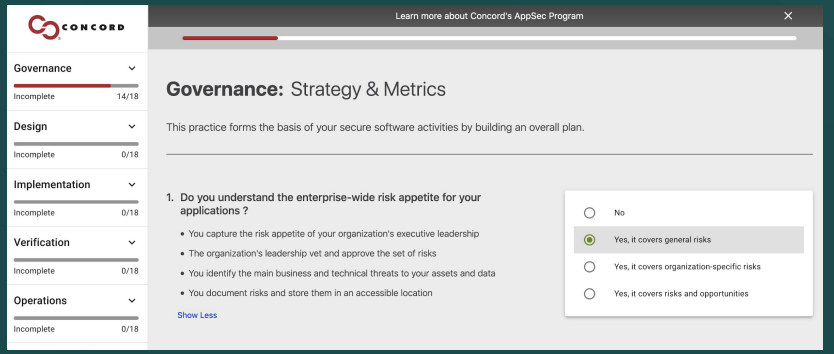
OWASP SAMM Assessment Toolbox

Tools of the trade

- SAMM 2.0 Calculator by Concord USA
- SAMM 2.0 Dashboard by SathIsh AshwIn
- OWASP Maturity Models
- OWASP SAMM Toolkit - GDocs version
- OWASP SAMM Assessment - Google Forms & Data Studio
- OWASP SAMM Toolkit - MS Excel

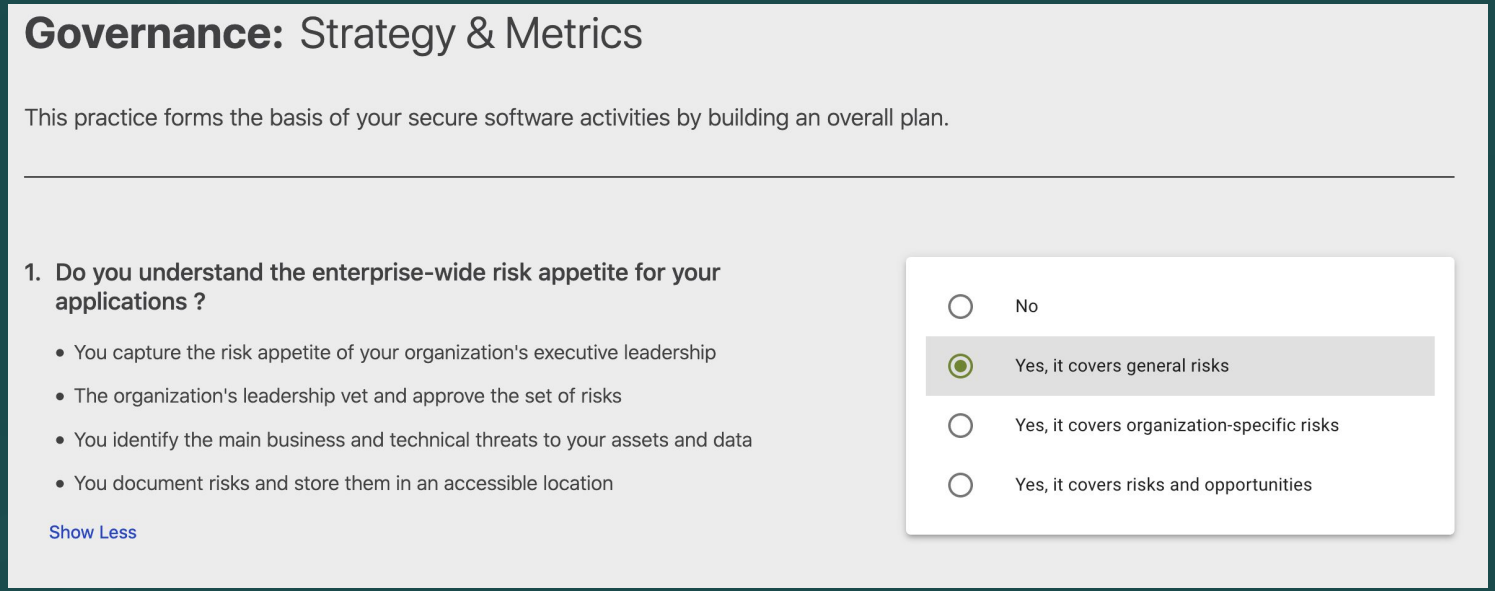
SAMM 2.0 Calculator: ConcordUSA

- Components:
  - Self-guided assessment
  - Function/Practice Breakdown
  - Function Maturity Breakdown
- SaaS Web-Based Tool
- Progress Bar
- Industry Benchmark Comparison
- Ready to use!



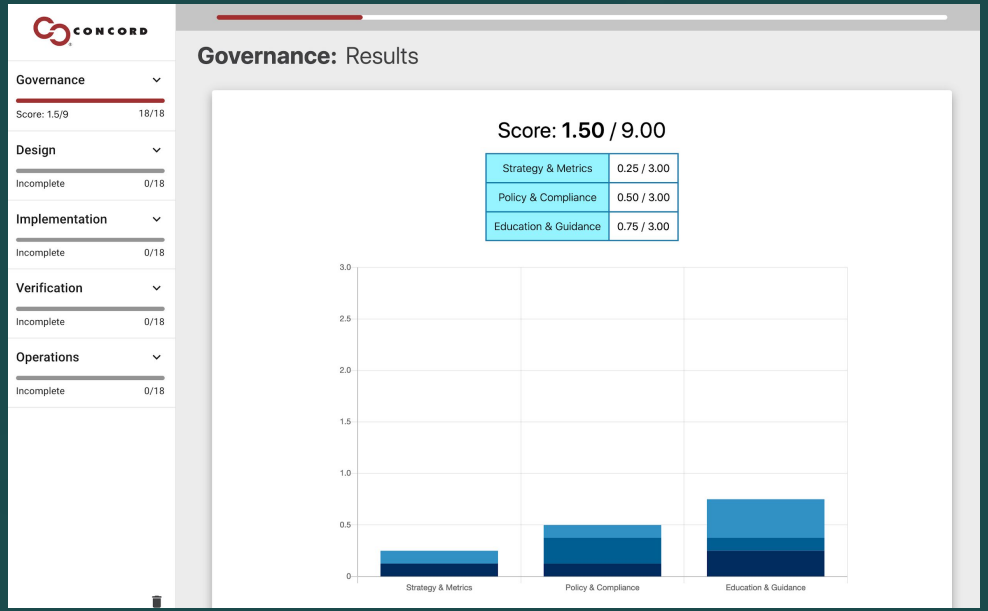
https://concordusa.com/SAMM/

SAMM 2.0 Calculator: ConcordUSA



https://concordusa.com/SAMM/

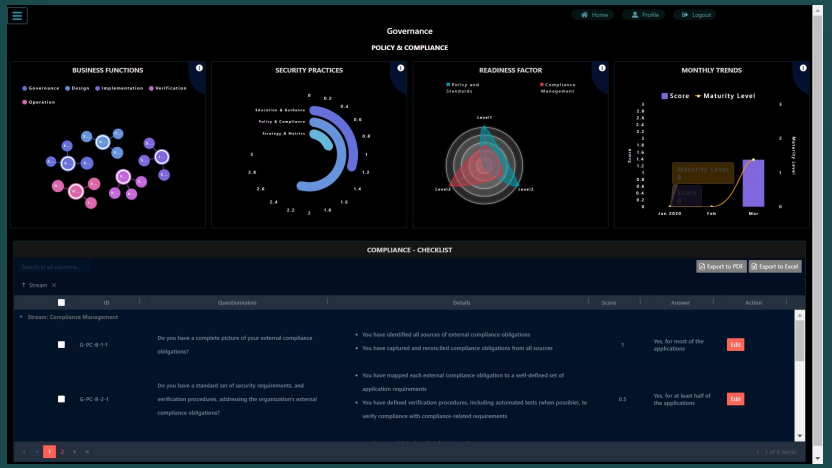
SAMM 2.0 Calculator: ConcordUSA



https://concordusa.com/SAMM/

SAMM 2.0 Dashboard

- Components:
  - Authenticated App
  - Role Based Access Control
  - Practice Trending
- Angular project on Github
- PDF/Excel Report Generation
- Self-Hosted Solution
- Ready to use!

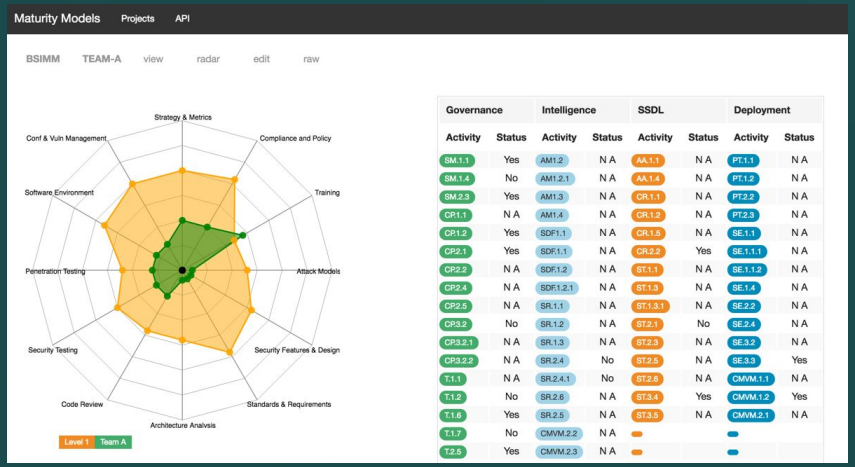


https://github.com/OWASP/samm/tree/master/Supporting%20Resources/app

OWASP
Open Web Application Security Project

OWASP Maturity Models

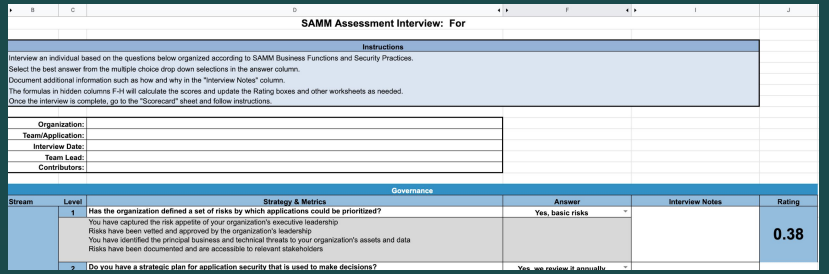
- Node project on Github
- BSIMM focus with future support for OWASP SAMM
- Self-Hosted Solution



https://github.com/owasp/Maturity-Models

Google Sheets

- Google Sheets Version of Excel Toolkit
- Can be exported to reporting tools and shared with others
- *Currently being validated!*



SAMM Assessment Interview: For

Instructions
Interview an individual based on the questions below organized according to SAMM Business Functions and Security Practices.
Select the best answer from the multiple choice drop down selections in the answer column.
Document additional information such as how and why in the "Interview Notes" column.
The formulas in hidden columns F-H will calculate the scores and update the Rating boxes and other worksheets as needed.
Once the interview is complete, go to the "Scorecard" sheet and follow instructions.

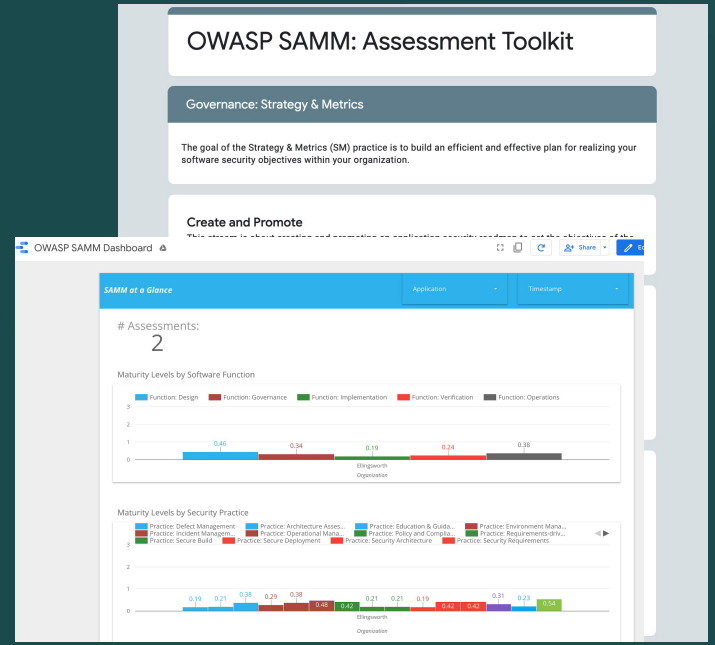
Organization:	
Team/Application:	
Interview Date:	
Team Lead:	
Contributors:	

Governance					
Stream	Level	Strategy & Metrics	Answer	Interview Notes	Rating
	1	Has the organization defined a set of risks by which applications could be prioritized?	Yes, basic risks		0.38
		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?	Yes, we review it annually		

https://docs.google.com/spreadsheets/d/1uBoiaHcY3UpdZim1zGuKkVwSxhmCHCnaq5nawnfglsY/edit?usp=sharing

Google Forms & Data Studio

- Google Sheets/Forms based assessment
  - Data is stored in Google Sheets
- Easy Self-service Form
- Responses can be edited
- Can be exported to reporting tools
  - Google Data Studio
- *Currently being validated!*



https://forms.gle/ufT6N79WFtoh2Bj66
https://datastudio.google.com/open/1R8vQxl13O6Qb42U-BOIMNLGRHIfR9qHA?usp=sharing

Part Two

OWASP SAMM Tools

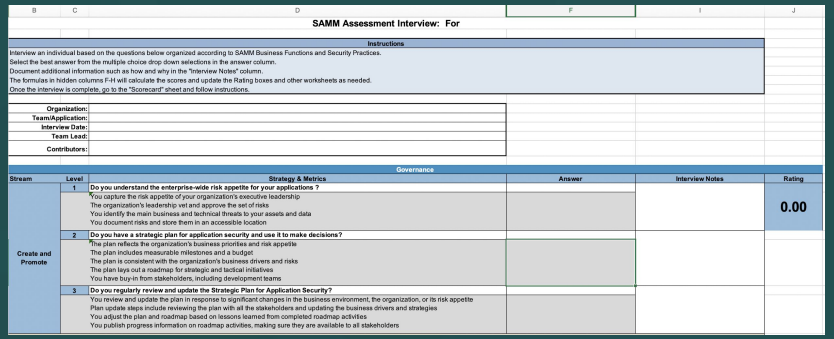
- Tools of the Trade
- *SAMM Assessment Toolkit*
- Benchmark Project
- Leveraging OWASP Projects & Tools

OWASP SAMM Toolkit - MS Excel

Features:

- Interview Template
- Assessment Questions (90)
- Quality Criteria
- Visual Maturity Scorecard
- Roadmap Phase Planner
- Roadmap Chart
- Maturity Rating Calculator

Ready to use!



SAMM Assessment Interview: For

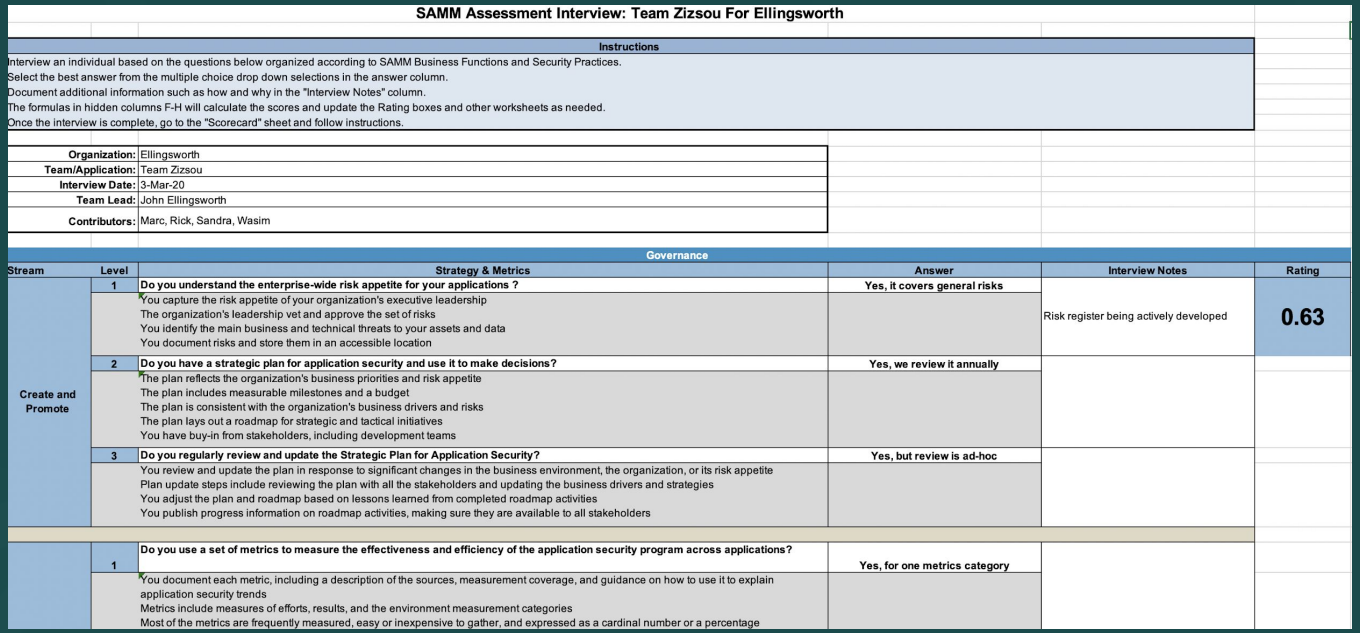
Instructions
Interview an individual based on the questions below organized according to SAMM Business Functions and Security Practices.
Select the best answer from the multiple choice drop down selections in the answer column.
Document additional information such as how and why in the "Interview Notes" column.
The formulas in hidden columns F-H will calculate the scores and update the Rating boxes and other worksheets as needed.
Once the interview is complete, go to the "Scorecard" sheet and follow instructions.

Organization:	
Team/Application:	
Interview Date:	
Team Lead:	
Contributors:	

Governance					
Stream	Level	Strategy & Metrics	Answer	Interview Notes	Rating
Create and Promote	1	Do you understand the enterprise-wide risk appetite for your applications ? 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			0.00
	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			

OWASP
Open Web Application Security Project

OWASP SAMM Toolkit - MS Excel



SAMM Assessment Interview: Team Zizsou For Ellingsworth

Instructions
Interview an individual based on the questions below organized according to SAMM Business Functions and Security Practices.
Select the best answer from the multiple choice drop down selections in the answer column.
Document additional information such as how and why in the "Interview Notes" column.
The formulas in hidden columns F-H will calculate the scores and update the Rating boxes and other worksheets as needed.
Once the interview is complete, go to the "Scorecard" sheet and follow instructions.

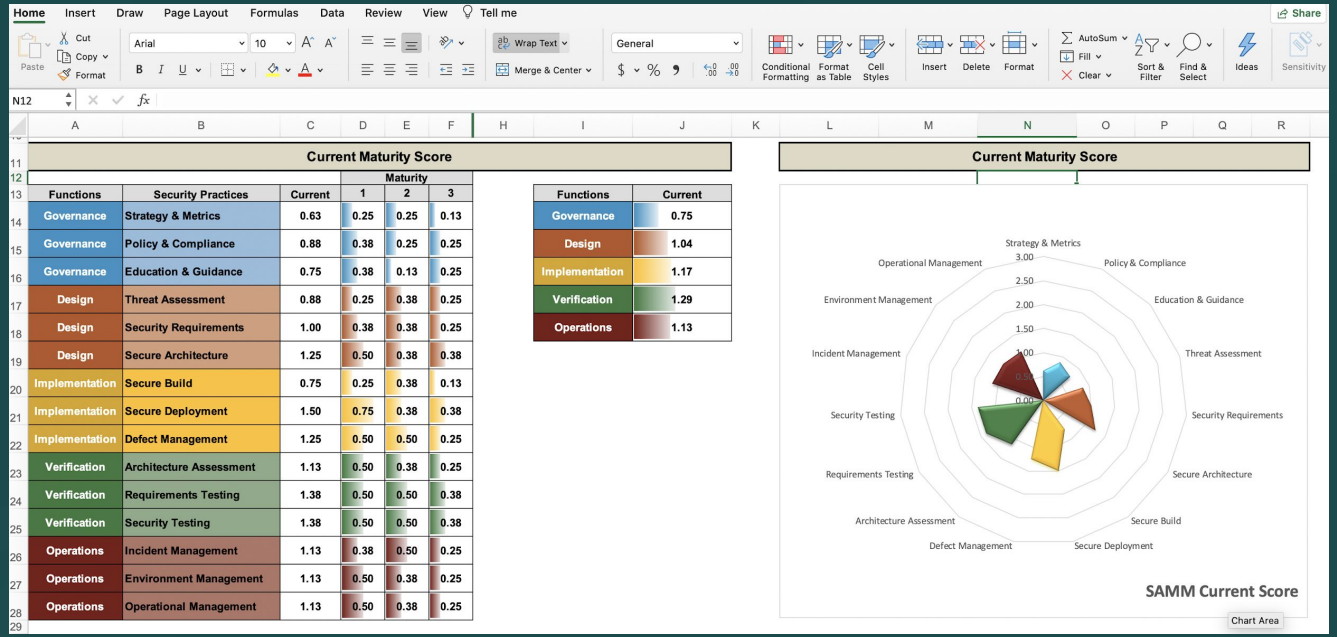
Organization:	Ellingsworth
Team/Application:	Team Zizsou
Interview Date:	3-Mar-20
Team Lead:	John Ellingsworth
Contributors:	Marc, Rick, Sandra, Wasim

Governance

Stream	Level	Strategy & Metrics	Answer	Interview Notes	Rating
Create and Promote	1	**Do you understand the enterprise-wide risk appetite for your applications ?**	**Yes, it covers general risks**	Risk register being actively developed	**0.63**
		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?**	**Yes, we review it annually**		
		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?**	**Yes, but review is ad-hoc**		
		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			
	1	**Do you use a set of metrics to measure the effectiveness and efficiency of the application security program across applications?**	**Yes, for one metrics category**		
		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			

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

OWASP SAMM Toolkit - MS Excel



Current Maturity Score

Functions	Security Practices	Current	Maturity 1	2	3
Governance	Strategy & Metrics	0.63	0.25	0.25	0.13
Governance	Policy & Compliance	0.88	0.38	0.25	0.25
Governance	Education & Guidance	0.75	0.38	0.13	0.25
Design	Threat Assessment	0.88	0.25	0.38	0.25
Design	Security Requirements	1.00	0.38	0.38	0.25
Design	Secure Architecture	1.25	0.50	0.38	0.38
Implementation	Secure Build	0.75	0.25	0.38	0.13
Implementation	Secure Deployment	1.50	0.75	0.38	0.38
Implementation	Defect Management	1.25	0.50	0.50	0.25
Verification	Architecture Assessment	1.13	0.50	0.38	0.25
Verification	Requirements Testing	1.38	0.50	0.50	0.38
Verification	Security Testing	1.38	0.50	0.50	0.38
Operations	Incident Management	1.13	0.38	0.50	0.25
Operations	Environment Management	1.13	0.50	0.38	0.25
Operations	Operational Management	1.13	0.50	0.38	0.25

Functions	Current
Governance	0.75
Design	1.04
Implementation	1.17
Verification	1.29
Operations	1.13

Current Maturity Score

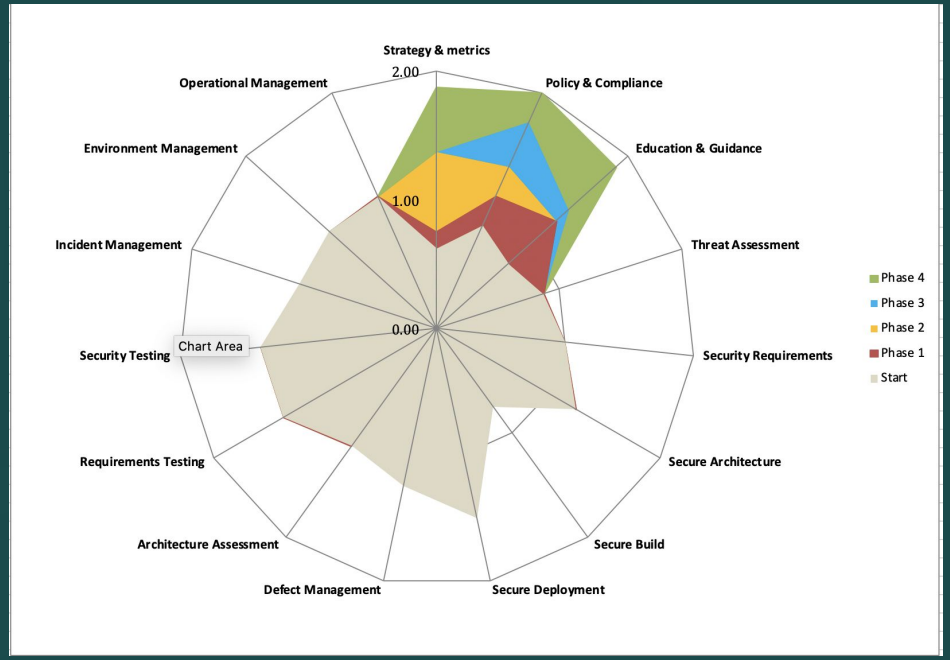
https://github.com/OWASP/samm/tree/master/Supporting%20Resources/v2.0/toolbox

OWASP SAMM Toolkit - MS Excel

F	I	J	M	N	Q	R	U	V	Y
Current		**Phase I**		**Phase II**		**Phase III**		**Phase IV**	
Answer	**Rating**	**Answer**	**Rating**	**Answer**	**Rating**	**Answer**	**Rating**	**Answer**	**Rating**
Yes, it covers general risks		Yes, it covers organization-specific risks		Yes, it covers organization-specific risks		Yes, it covers organization-specific risks		Yes, it covers risks and opportunities	
Yes, we review it annually		Yes, we review it annually		Yes, we consult the plan before making significant decisions		Yes, we consult the plan before making significant decisions		Yes, we consult the plan before making significant decisions	
Yes, but review is ad-hoc		Yes, but review is ad-hoc		Yes, we review it at regular times		Yes, we review it at regular times		Yes, we review it at regular times	
	0.63		**0.75**		**1.38**		**1.38**		**1.88**
Yes, for one metrics category		Yes, for two metrics categories		Yes, for two metrics categories		Yes, for two metrics categories		Yes, for all three metrics categories	
Yes, for some of the metrics		No		Yes, for at least half of the metrics		Yes, for at least half of the metrics		Yes, for at least half of the metrics	
No		No		Yes, but review is ad-hoc		Yes, but review is ad-hoc		Yes, but review is ad-hoc	
Answer	**Rating**	**Answer**	**Rating**	**Answer**	**Rating**	**Answer**	**Rating**	**Answer**	**Rating**
for at least half of the applications		Yes, for most or all of the applications		Yes, for most or all of the applications		Yes, for most or all of the applications		Yes, for most or all of the applications	
Yes, some content		Yes, some content		Yes, at least half of the content		Yes, most or all of the content		Yes, most or all of the content	
Yes, but reporting is ad-hoc	**0.88**	Yes, but reporting is ad-hoc	**1.13**	Yes, but reporting is ad-hoc	**1.38**	Yes, but reporting is ad-hoc	**1.75**	Yes, we report at regular times	**2.00**
Yes, for some applications		Yes, for some applications		Yes, for some applications		Yes, for some applications		Yes, for at least half of the applications	
Yes, for some obligations		Yes, for some obligations		Yes, for at least half of the obligations		Yes, for at least half of the obligations		Yes, for at least half of the obligations	
Yes, but reporting is ad-hoc		Yes, but reporting is ad-hoc		Yes, but reporting is ad-hoc		Yes, we report at regular times		Yes, we report at regular times	
Answer	**Rating**	**Answer**	**Rating**	**Answer**	**Rating**	**Answer**	**Rating**	**Answer**	**Rating**
Yes, at least half of them		Yes, most or all of them		Yes, most or all of them		Yes, most or all of them		Yes, most or all of them	
Yes, for some of the training		Yes, for at least half of the training		Yes, for at least half of the training		Yes, for at least half of the training		Yes, for most or all of the training	
Yes, for some of the training	**0.88**	Yes, for some of the training	**1.25**	Yes, for some of the training	**1.25**	Yes, for some of the training	**1.38**	Yes, for some of the training	**1.88**
Yes, for some teams		Yes, for some teams		Yes, for some teams		Yes, for at least half of the teams		Yes, for most or all of the teams	
Yes, we started implementing it		Yes, we started implementing it		Yes, we started implementing it		Yes, we started implementing it		Yes, we started implementing it	
Yes, we started implementing it		Yes, we started implementing it		Yes, we started implementing it		Yes, we started implementing it		Yes, we started implementing it	

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

OWASP SAMM Toolkit - MS Excel



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

Part Two

OWASP SAMM Tools

- Tools of the Trade
- SAMM Assessment Toolkit
- *Benchmark Project*
- Leveraging OWASP Projects & Tools

Benchmark Project

Business Wire
A Berkshire Hathaway Company

HOME SERVICES NEWS EDUCATION ABOUT US

Search

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-

OWASP
Open Web Application Security Project

OWASP SAMM Benchmark Project

Overview

- An open model for security benchmarking
- Consortium of security companies working together
- Confidentiality maintained between client & security company
- Public data anonymized for benchmarking between teams, organizations

OWASP SAMM Benchmark Project

Benefits

- Validate transformation plans
- Supporting existing plans
- Clients of various security companies can utilize platform
- Find specific maturities in teams and organizations with varying granularity
- Bring security maturity testing to the masses

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**

Part Two

OWASP SAMM Tools

- Tools of the Trade
- SAMM Assessment Toolkit
- Benchmark Project
- *Leveraging OWASP Projects & Tools*

150+ OWASP Projects

PROTECT

Tools: AntiSamy Java/:NET, Enterprise Security API (ESAPI), ModSecurity Core Rule Set Project

Docs: Development Guide, .NET, Ruby on Rails Security Guide, Secure Coding Practices - Quick Reference Guide

DETECT

Tools: JBroFuzz, Lice CD, WebScarab, Zed Attack Proxy

Docs: Application Security Verification Standard, Code Review Guide, Testing Guide, Top Ten Project

LIFE CYCLE

SAMM, WebGoat, Legal Project

Day 2 Schedule

Part Three

Applying OWASP SAMM

- Methodology
- Establishing Assessment Scope
- Assessing Governance
- Assessing Design
- Assessing Implementation
- Assessing Verification
- Assessing Operations
- Setting Maturity Targets & Improvement Activities

Part Four

OWASP SAMM Best Practices

- Choosing the Right Starting Points
- Metrics and Management
- Achieving Security by Design
- Critical Success Factors

Day 1 Recap

Part One

SDLC Overview & OWASP SAMM Introduction

- The Application Security Challenge
- Software Development Lifecycle (SDLC) Overview
- OWASP SAMM - Vision, History, Structure
- OWASP SAMM As an Assessment Tool

Part Two

OWASP SAMM Tools

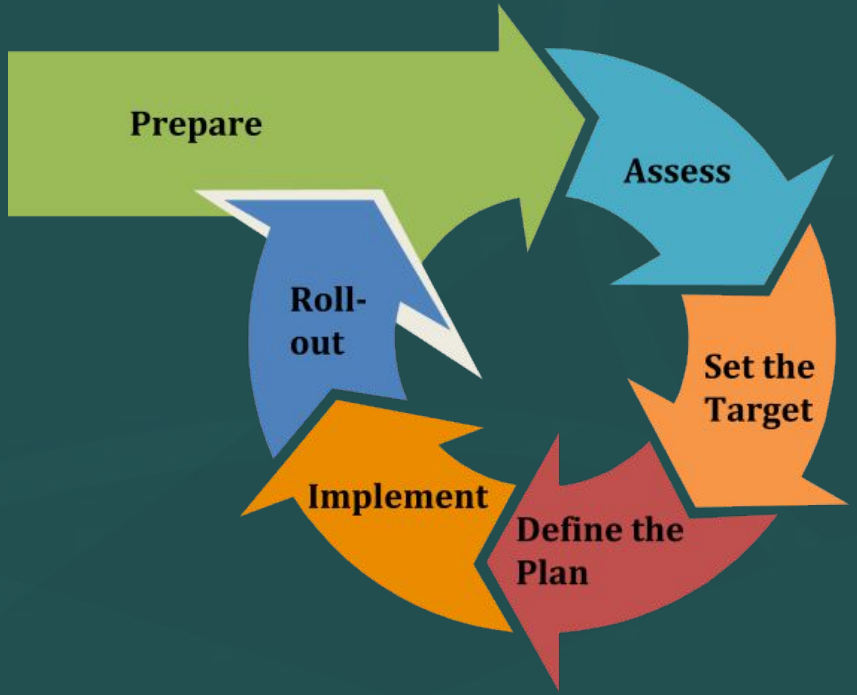
- Tools of the Trade
- SAMM Assessment Toolkit
- Benchmark Project
- Leveraging OWASP Projects and Tools

Part Three

Applying OWASP SAMM

- *Methodology*
- Establishing Assessment Scope
- Assessing Governance
- Assessing Design
- Assessing Implementation
- Assessing Verification
- Assessing Operations
- Setting Improvement Targets

Methodology: Adaptable Approach



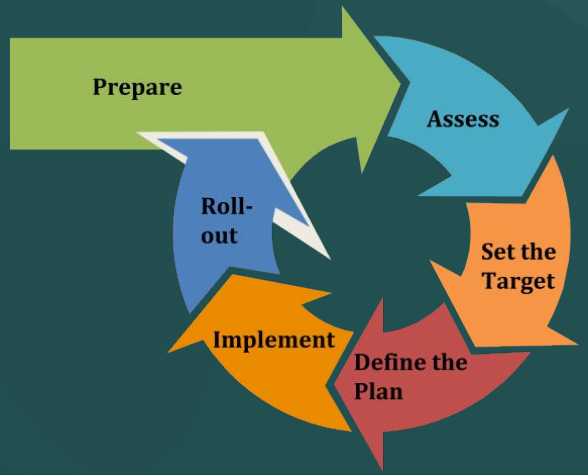
Prepare

Purpose

- Ensure a proper start of the project

Activities

- Define the scope (uniform unit(s))
- Identify stakeholders
- Socialize – spread the word!



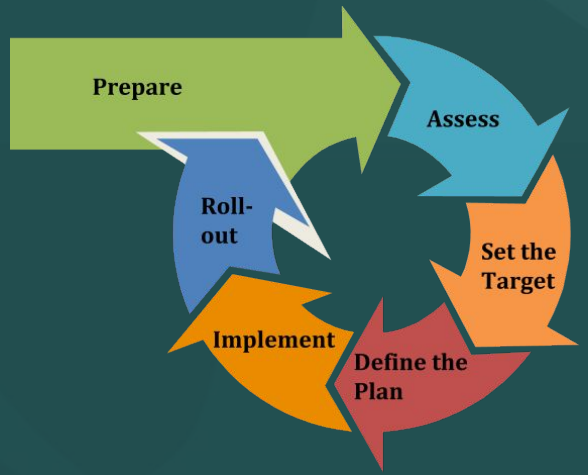
Assess

Purpose

- Identify and understand the maturity of the 15 practices for the chosen scope

Activities

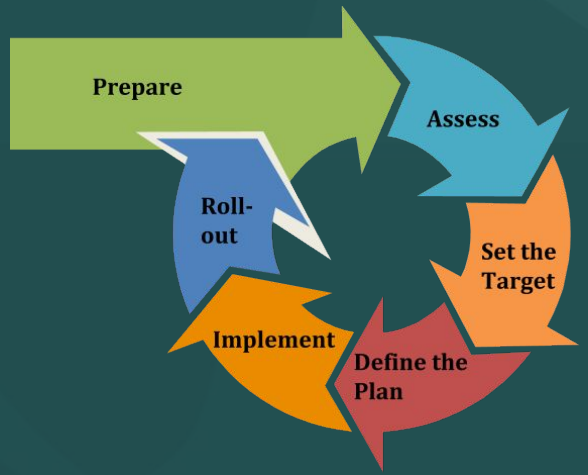
- Evaluate current practices
- Determine maturity level



Set the Target

Purpose

- Develop a target score to guide you in future improvements



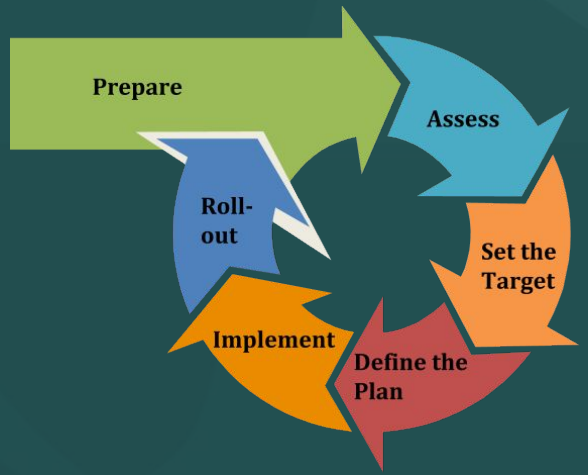
Activities

- Define the target
- Estimate overall impact

Define the Plan

Purpose

- Define or update the plan to take you to the next level



Activities

- Determine change schedule
- Develop/update the roadmap plan

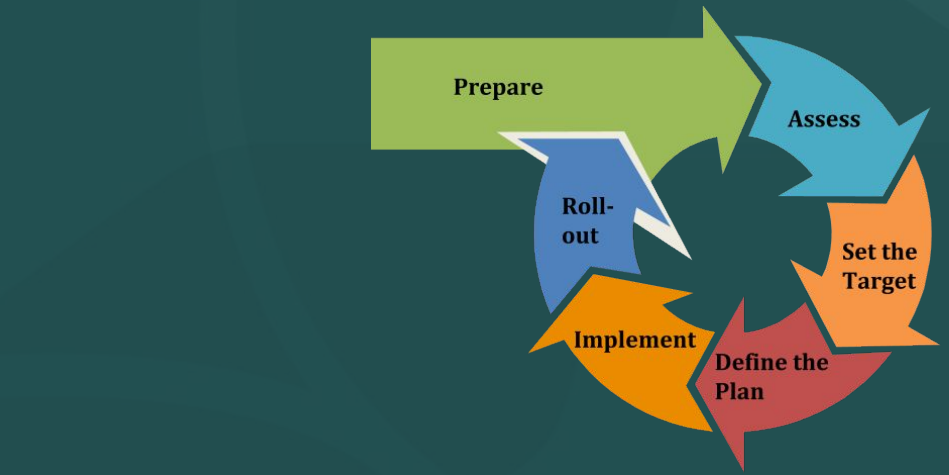
Implement

Objective

- Work the plan

Activities

- Implement activities



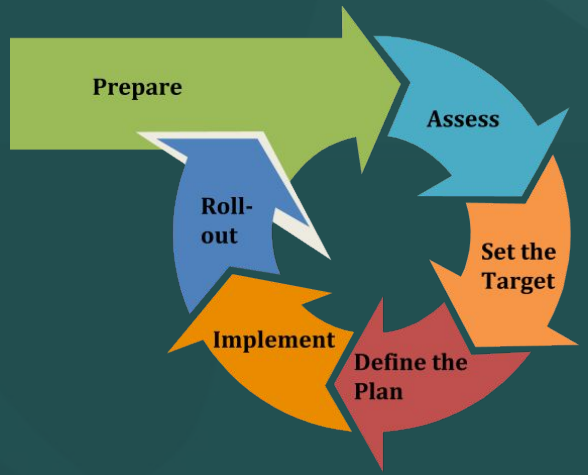
Roll-Out

Objective

- Ensure improvements are available and effectively used

Activities

- Evangelize improvements
- Measure effectiveness



Part Three

Applying OWASP SAMM

- Methodology
- *Establishing Assessment Scope*
- Assessing Governance
- Assessing Design
- Assessing Implementation
- Assessing Verification
- Assessing Operations
- Setting Improvement Targets

Establishing Assessment Scope

Scope based on Organization structure:

- Organization wide
- Selected Business Units/Center of Excellence
- Development Groups (internal, supplier)
- IT infrastructure Groups (hosting internal, cloud)

Scope based on Application risk profile:

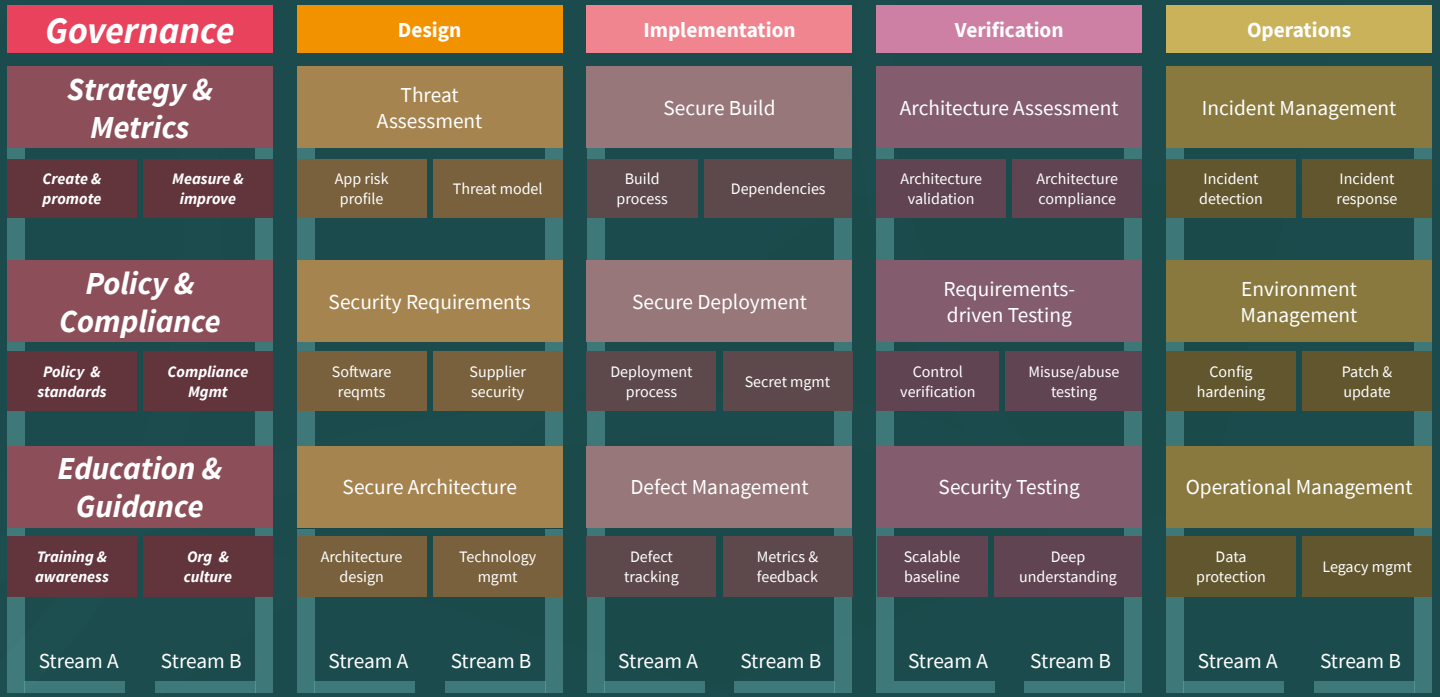
- High, Medium, Low based on risk: e.g. Internet facing, transactional, etc.
- Data Classification level: e.g. Confidential, sensitive, public

Part Three

Applying OWASP SAMM

- Methodology
- Establishing Assessment Scope
- *Assessing Governance*
- Assessing Design
- Assessing Implementation
- Assessing Verification
- Assessing Operations
- Setting Improvement Targets

Governance Business Function



OWASP
Open Web Application Security Project

Strategy & Metrics

Goal is to build an efficient and effective plan for realizing your software security objectives within your organization

- Forms the basis of your secure software activities by building an overall plan.
- Driver for all other OWASP SAMM practices

Characteristics:

- Measurable
- Aligned with business risk
- Continuous improvement

Strategy & Metrics

Do you understand the enterprise-wide risk appetite for your applications?

- No
- Yes, it covers general risks
- Yes, it covers organization-specific risks
- Yes, it covers risks and opportunities

- 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

Policy & Compliance

Goal is to understand and adhere to legal and regulatory requirements

- Internal standards as well as 3rd party requirements
- Both Security and Privacy are critical

Technical standards become more important

- They are an important driver for software security requirements

Often a very informal practice in organisations

Policy & Compliance

Do you have and apply a common set of policies and standards throughout your organization?

- No
- Yes, for some applications
- Yes, for at least half of the applications
- Yes, for most or all of the applications

- You have adapted existing standards appropriate for the organization's industry to account for domain- specific considerations
- Your standards are aligned with your policies and incorporate technology-specific implementation guidance

Education & Guidance

Goal is to disseminate security-oriented information to *all* stakeholders involved in the software development lifecycle

Security to be integrated in organisation **training** curriculum

- An ounce of effort is not sufficient
- Teach teams to be security self-sufficient

Work on the organisational habits via security **culture**

- Important element of a successful software assurance project

Education & Guidance

Do you require employees involved with application development to take SDLC training?

- No
- Yes, some of them
- Yes, at least half of them
- Yes, most or all of them

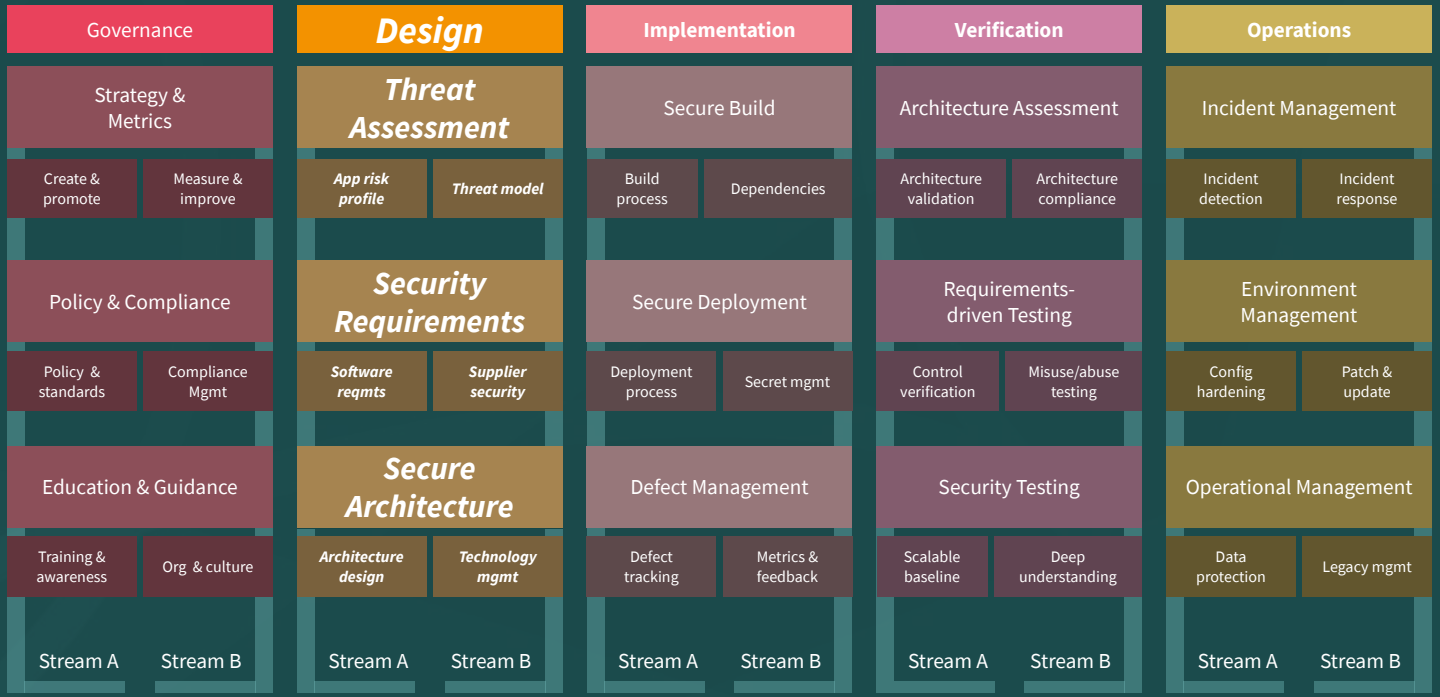
- Training is repeatable, consistent, and available to all stakeholders
- Training includes the latest OWASP Top 10
- Training requires a sign-off or an acknowledgement from attendees
- Training is updated annually
- Training is required during onboarding

Part Three

Applying OWASP SAMM

- Methodology
- Establishing Assessment Scope
- Assessing Governance
- *Assessing Design*
- Assessing Implementation
- Assessing Verification
- Assessing Operations
- Setting Improvement Targets

Design Business Function



OWASP
Open Web Application Security Project

Threat Assessment

Analyze the risks of the application

- from a business perspective, via *risk profiles*
- from a technical perspective, via *threat modeling*

Threat modeling is where “the magic” kicks in determining:

- What are we building?
- What could go wrong?
- How will we prevent it?
- Did what we do work?
- Your imagination is the limit

Threat Assessment

Do you classify applications according to business risk based on a simple and predefined set of questions?

- No
- Yes, some of them
- Yes, at least half of them
- Yes, most or all of them

- An agreed-upon risk classification exists
- The application team understands the risk classification
- The risk classification covers critical aspects of business risks the organization is facing
- The organization has an inventory for the applications in scope

Security Requirements

Goal is to make security specification more explicit

Turn security into a positively-spaced problem

Security requirements sources:

- Compliance
- Standards
- Functionality
- Quality

Requirements should be specified in a S.M.A.R.T. way

Also look into how suppliers approach to security

Security Requirements

Do project teams specify security requirements during development?

- No
- Yes, for some applications
- Yes, for at least half of the applications
- Yes, for most or all of the applications

- Teams derive security requirements from functional requirements and customer or organization concerns
- Security requirements are specific, measurable, and reasonable
- Security requirements are in line with the organizational baseline

Secure Architecture

Secure Architecture is a key practice for security. Poor decisions at this step can have major impact, and are often difficult (and potentially *costly*) to fix.

Software Architecture components

- Ensure that the architecture contains proper elements to meet the security requirements

Supporting Technology

- Verify that development stacks, deployment tools and other supporting technology are in-line with security expectations

Secure Architecture

Do teams use security principles during design?

- No
- Yes, for some applications
- Yes, for at least half of the applications
- Yes, for most or all of the applications

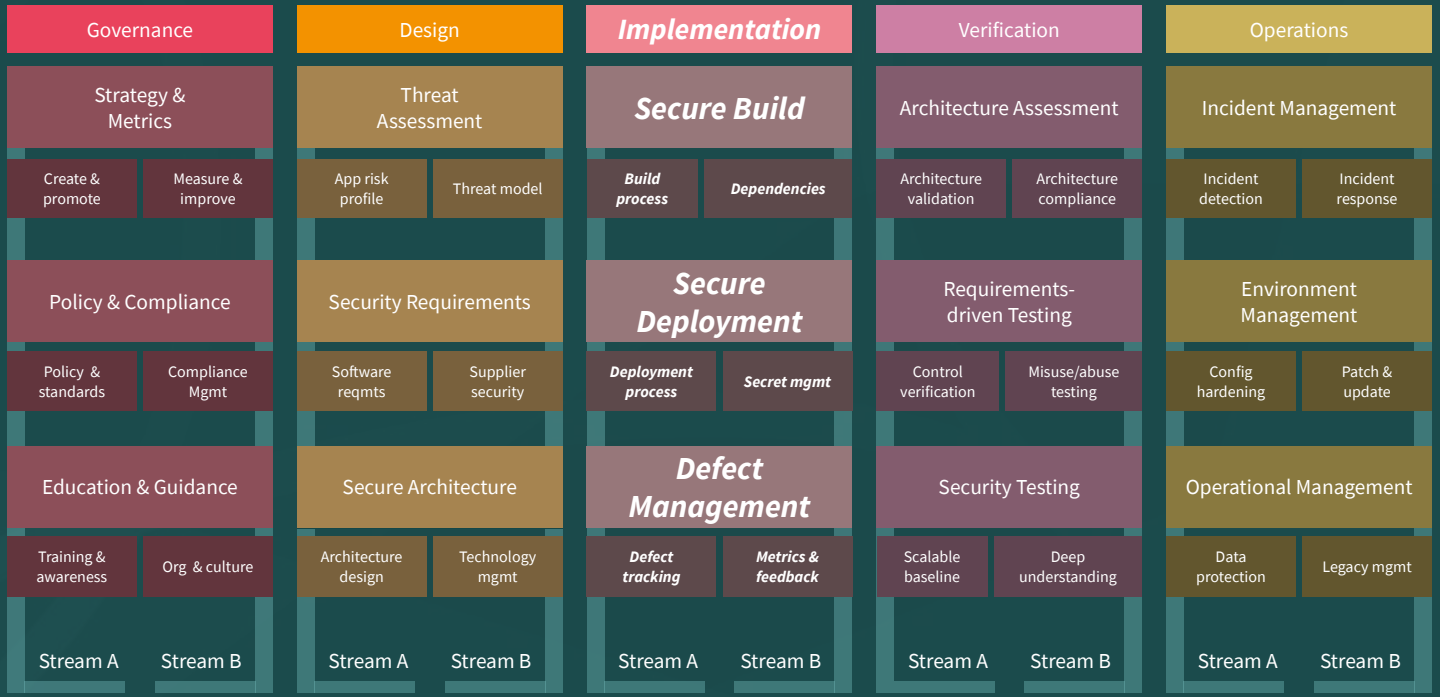
- You have an agreed upon checklist of security principles
- You store your checklist in an accessible location
- Relevant stakeholders understand security principles

Part Three

Applying OWASP SAMM

- Methodology
- Establishing Assessment Scope
- Assessing Governance
- Assessing Design
- *Assessing Implementation*
- Assessing Verification
- Assessing Operations
- Setting Improvement Targets

Implementation Business Function



OWASP
Open Web Application Security Project

Secure Build

Secure build focuses on using a reliable production process in order to generate secure software artifacts and to avoid issues being introduced during the process

An important part is the build process itself, where the goal is consistent, repeatable, and automated

A second part focuses on software dependencies or 3rd party libraries, aka supply chain security.

Secure Build

Is your full build process formally described?

- No
- Yes, for some applications
- Yes, for at least half of the applications
- Yes, for most or all of the applications

- You have enough information to recreate the build processes
- Your build documentation up to date
- Your build documentation is stored in an accessible location
- Produced artifact checksums are created during build to support later verification
- You harden the tools that are used within the build process

Secure Deployment

One of the final stages in delivering secure software is ensuring the security and integrity of developed applications are not compromised during their deployment.

- In the deployment process, appropriate protections are a repeatable deployment process, separation of duties, etc.
- All secrets required for the software to run must be properly protected for deployment and during execution. Tools such as password vaults can help to achieve this.

Secure Deployment

Do you use repeatable deployment processes?

- No
- Yes, for some applications
- Yes, for at least half of the applications
- Yes, for most or all of the applications

- You have enough information to run the deployment processes
- Your deployment documentation up to date
- Your deployment documentation is accessible to relevant stakeholders
- You ensure that only defined qualified personnel can trigger a deployment
- You harden the tools that are used within the deployment process

Defect Management

The Defect Management practice focuses on collecting, recording, and analysing software security defects and enriching them with information to drive metrics-based decisions.

It is a central funnel for all defects identified in other security practices.

- A defect tracking solution helps the organization to keep track of identified problems, and to manage them in a controlled manner.
- Analysis of defects supported by metrics can help to increase awareness and guide improvement programs in the organization.

Defect Management

Do you track all known security defects in accessible locations?

- No
- Yes, for some applications
- Yes, for at least half of the applications
- Yes, for most or all of the applications

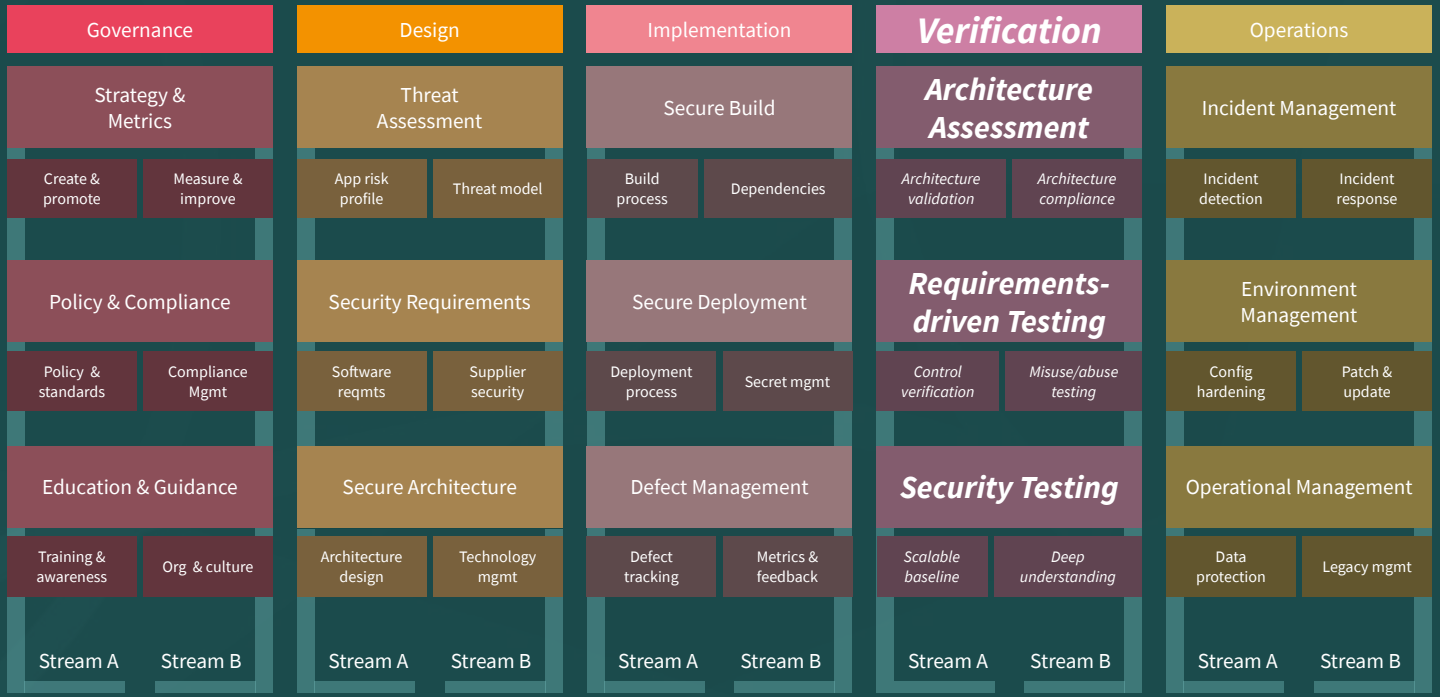
- You can easily get an overview of all security defects impacting one application
- You have at least a rudimentary classification scheme in place
- The process includes a strategy for handling false positives and duplicate entries
- The defect management system covers defects from various sources and activities

Part Three

Applying OWASP SAMM

- Methodology
- Establishing Assessment Scope
- Assessing Governance
- Assessing Design
- Assessing Implementation
- *Assessing Verification*
- Assessing Operations
- Setting Improvement Targets

Verification Business Function



OWASP
Open Web Application Security Project

Architecture Assessment

Verify whether the solution meets security and compliance requirements

Covers both software and supporting infrastructure

Rigorous inspection of data flows & security mechanisms

Architecture Assessment

Do you review the application architecture for key security objectives on an ad-hoc basis?

- No
- Yes, for some applications
- Yes, for at least half of the applications
- Yes, for most or all of the applications

- You have an agreed upon model of the overall software architecture
- You include components, interfaces, and integrations in the architecture model
- You verify the correct provision of general security mechanisms
- You log missing security controls as defects

Requirements-driven Testing

First perspective for testing: *test the software according to the requirements*

- Conduct positive and negative security tests to verify that the software operates as specified.
- From the known security requirements, identify and implement a set of security test cases to check the software for correct functionality.
- Use abuse testing for an application to run concrete security tests that directly or indirectly exploit identified abuse scenarios.
- Automate security testing (for each release) via security test automation and automated regression testing

Requirements-driven Testing

Do you test applications for the correct functioning of standard security controls?

- No
- Yes, some of them
- Yes, at least half of them
- Yes, most or all of them

- Security testing at least verifies the implementation of authentication, access control, input validation, encoding and escaping data, and encryption controls
- Security testing executes whenever the application changes its use of the controls

Security Testing

Second perspective for testing: *test the software according to security best practices*

- SAST/DAST/IAST automated tooling
- Manual testing for fine-grained verification
- Detected defects will require validation, risk analysis & recommendations to fix

Security Testing

Do you scan applications with automated security testing tools?

- No
- Yes, some of them
- Yes, at least half of them
- Yes, most or all of them

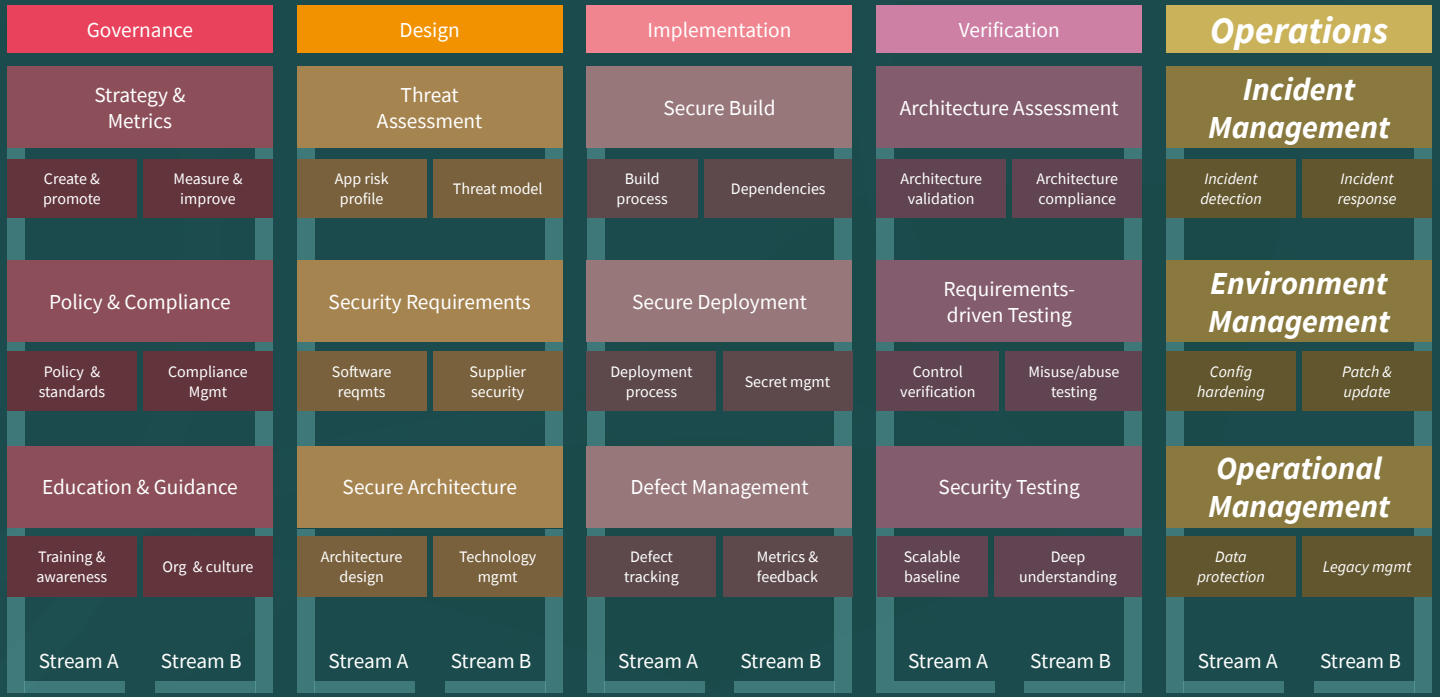
- You dynamically generate inputs for security tests using automated tools
- You choose the security testing tools to fit the organization's architecture and technology stack, and balance depth and accuracy of inspection with usability of findings to the organization

Part Three

Applying OWASP SAMM

- Methodology
- Establishing Assessment Scope
- Assessing Governance
- Assessing Design
- Assessing Implementation
- Assessing Verification
- *Assessing Operations*
- Setting Improvement Targets

Operations Business Function



OWASP
Open Web Application Security Project

Incident Management

Prepare for WHEN, not IF!

Examples of a security incidents:

- successful DoS (Denial of Service) attack against a cloud application
- application user accessing private data of another one by abusing a security vulnerability
- attacker modifying the application source code

Have a capability in place to **detect** potential incidents

Make sure you can **respond** to detected incidents

Use vulnerability metrics and root-cause analysis to improve SDLC

Incident Management

Do you analyze log data for security incidents periodically?

- No
- Yes, for some applications
- Yes, for at least half of the applications
- Yes, for most or all of the applications

- You have a contact point for the creation of security incidents
- You analyze data in accordance with the log data retention periods
- The frequency of this analysis is aligned with the criticality of your applications

Environment Management

Application security transitions to operational modes. New security features and patches are continuously released until the technology stack you're using becomes obsolete.

Pro-actively **maintain** the different technology components in the software environment by activating security features and removing unnecessary ones.

Install **patches** to ensure technology components can withstand known security attacks.

Environment Management

Do you harden configurations for key components of your technology stacks?

- No
- Yes, for some components
- Yes, for at least half of the components
- Yes, for most or all of the components

- You have identified the key components in each technology stack used
- You have an established configuration standard for each key component

Operational Management

This practice focuses on operational support activities required to maintain security throughout the product lifecycle.

Data must be sufficiently **protected** in its different forms and environments to ensure a correct operation of the application

Legacy management ensures there are no loose ends, often forgotten, in the organisation which may form an easy target to attackers.

Operational Management

Do you identify and patch vulnerable components?

- No
- Yes, for some components
- Yes, for at least half of the components
- Yes, for most or all of the components

- You have an up-to-date list of components, including version information
- You regularly review public sources for vulnerabilities related to your components

Part Three

Applying OWASP SAMM

- Methodology
- Establishing Assessment Scope
- Assessing Governance
- Assessing Design
- Assessing Implementation
- Assessing Verification
- Assessing Operations
- *Setting Improvement Targets*

Setting Improvement Targets

Roadmap templates can provide direction for targets

- *What type of company are you ?*

Take into account the company's risk appetite

Only include activities where you see added value for the company, even for lower levels

OWASP SAMM activities have dependencies – use them !

Think about links with other practices in the company e.g., training, release management, risk management,

Sample Roadmap

Source Data	As-Is				To-Be
Security Practices/Phase	**Start**	**Phase 1**	**Phase 2**	**Phase 3**	**Phase 4**
Strategy & metrics	1.63	1.88	2.00	2.13	2.38
Policy & Compliance	1.13	1.13	1.38	1.63	2.13
Education & Guidance	1.25	1.25	1.25	1.25	1.25
Threat Assessment	1.25	1.25	1.25	1.25	1.25
Security Requirements	1.75	1.75	1.75	1.75	1.75
Secure Architecture	1.38	1.38	1.38	1.38	1.38
Secure Build	1.50	1.63	1.75	2.00	2.00
Secure Deployment	1.50	1.50	1.50	1.50	1.50
Defect Management	1.75	1.88	2.00	2.25	2.25
Architecture Assessment	2.00	2.00	2.00	2.00	2.00
Requirements Driven Tes	1.63	1.63	1.63	1.63	1.63
Security Testing	1.88	1.75	1.75	1.75	1.75
Incident Management	0.75	0.75	0.75	0.75	0.75
Environment Managemen	1.63	1.63	1.63	1.63	1.63
Operational Enablement	0.75	0.75	0.75	0.75	0.75
SAMM velocity:		0.38	0.63	0.88	0.75
		14%	24%	33%	29%

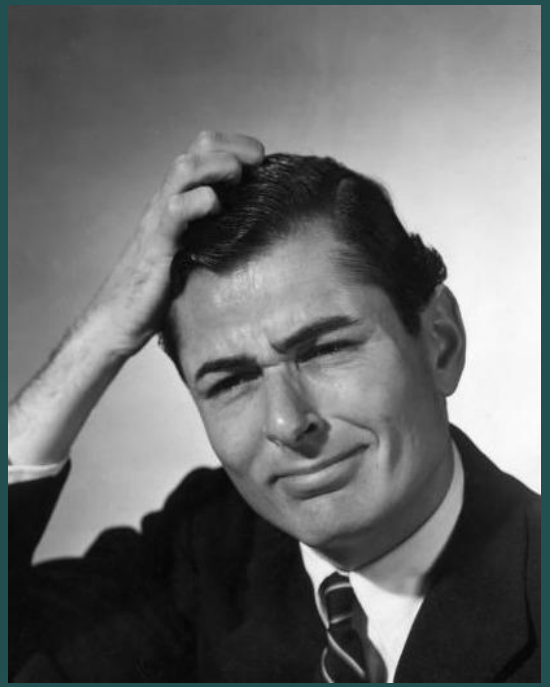
Part Four

OWASP SAMM Best Practices

- *Choosing the Right Starting Points*
- Metrics and Management
- Achieving Security by Design
- Critical Success Factors

Complicating Factors, Anyone ?

- Different development teams
- Different technology stacks
- Business-IT alignment issues
- Outsourced development



Start Where You Are

- Organizational Context
  - Be aware of assumptions about security, and work to alter them
- Realistic Goals
  - Focus on reasonable security outcomes
- Manageable Scope
- Constraints:
  - budget, timing, resources

What's Your Company Maturity ?

In terms of IT Strategy and application Landscape
In terms of Software Development practices

- Analysis, Design, Implementation, Testing, Release, Maintenance
- Structured vs. ad-hoc development

In terms of ITSM practices

- Configuration, Change, Release, Vulnerability-Management

Current Company Maturity ≈ *Feasibility of SDLC Program*

Importance of Business Case

If you want your security posture to improve, management buy-in is crucial!

⇒ You will need a business case to convince them

Typical arguments:

- Improved security quality
- Better cost efficiency
- Compliance
- Risk management
- Customer satisfaction
- Reputation management

Entry Points

Pick the weak spots that can demonstrate short-term ROI

Typical examples

- Awareness training
- Coding Guidelines
- External Pentesting

Success will help you in continuing your effort

Application Categorization

Use risk profiles to rationalize security effort and for prioritization

Data Classification

Integrations & dependencies

Communication & Support

Critical success factor

- Spreading the message to a broad audience
- Setup a secure applications portal !
- Regular status updates towards management

Part Four

OWASP SAMM Best Practices:

- Choosing the Right Starting Points
- *Metrics and Management*
- Achieving Security by Design
- Critical Success Factors

Metrics and Management

Success metrics are possible in SAMM for:

- 5 Business Functions
- 15 Security Practices
- 30 Streams
- 90 Activities

Leveraging a phased roadmap, there is plenty of time-based data to report progress, ROI, and success!

Metrics and Management

Application Metrics

- number of applications
- number of components by category of origin (COTS, GOTS, OSS, and so forth)
- counts of defects, weaknesses, or vulnerabilities
- effort fixing defects, weaknesses, and vulnerabilities
- effort applying or implementing security-related tools and techniques
- mean time to remediation
- ratio of defects or vulnerabilities found in production vs. test
- potential severity of the defect (CVSS, DREAD, etc.)

Metrics and Management

Process Metrics

- techniques used during each development activity
- effort fixing defects, weaknesses, and vulnerabilities
- effort applying security-related tools and techniques
- test effort and duration
- rate of weakness (or defect) removal

Responsibilities

Core Security team

- Support vs. Responsible role

Security Satellite

- Analysts
- Architects
- Developers
- Operations
- Management

Formalized RACI is possible but will be a challenge

Part Four

OWASP SAMM Best Practices:

- Choosing the Right Starting Points
- Metrics and Management
- *Achieving Security by Design*
- Critical Success Factors

The Power of Default Security

Implement development frameworks that are secure by default

Minimizes work for developers

Will lower number of vulnerabilities

Part Four

OWASP SAMM Best Practices

- Choosing the Right Starting Points
- Monitoring and Metrics
- Achieving Security by Default
- *Critical Success Factors*

Critical Success Factors

- Get initiative 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

SDLC Cornerstones – Recap

Conclusions

Developing secure software is increasingly complex

OWASP SAMM 2.0 is a global maturity foundation for software assurance, in line with current trends and practices

Applying OWASP SAMM:

- Assessment
- Roadmap
- (Continuous) Implementation

Be ready to face the organisational challenges that will pop up during the journey!

Current Roadmap

2020

- Iterative releases
  - v2.1
  - v2.2
- Agile/Devops guidance
- Roadshows/Trainings

Looking forward

- OWASP Project Integration
- Online assessments integrated with benchmark data
- User community contributions
- Support for regulations
- OWASP SAMM user summits
- Translations!

Support OWASP SAMM

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

Get Involved

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

SAMM Newsletter

OWASP
Open Web Application Security Project

OWASP
Open Web Application
Security Project

OWASP
SAMM

Questions?
Feedback?

OWASP
Open Web Application
Security Project

Thank you!