SAMM User Day Lisbon 2024

OWASP SAMM:

From zero to hero

Nariman Aga-Tagiyev
June 26th

SAMM assessments are the easy part

Agenda

1. Getting ready
2. Kick off
3. Assessments
4. Roadmap
5. Tools & Processes
6. Effects on the culture

1

Getting ready

Maturity Frameworks

Structured frameworks to evaluate and enhance security across business functions. These frameworks also aid in documenting the Software Security Development Lifecycle (SSDL) in a structured way.

OWASP SAMM

BSIMM

Let’s see Who’s Who

COMPETE AGAINST EXISTING POLICIES

SSDLC Policy

NIST CSF

SOC

ISO

COMPETE AGAINST EXISTING POLICIES

SSDLC Policy

OWASP SAMM is a Community

OWASP SAMM Community Call
Every second Wednesday
21:30 CEST

I wish you were more assertive

1. Courage
2. Commitment
3. Capabilities
4. [✓ Confidence]

Regroup and attack

OWASP SAMM is the way to go

- It’s about where you want to be and how to get there!
- Tailored roadmap per software factory
- Convertible to other frameworks thanks to the OpenCRE and NIST CSF <-> SAMM projects

2

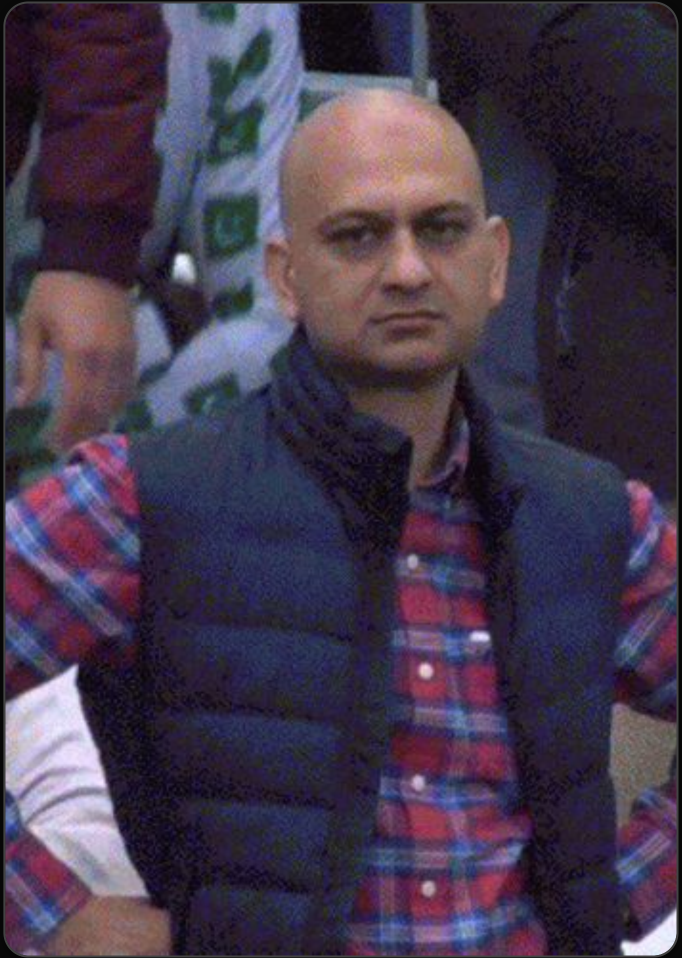
Kick off

Where do we start?

GLOBAL SSDLC

Perfect World Scenario

Secure Software Development Lifecycle policies usually represent
the target situation in big organizations.

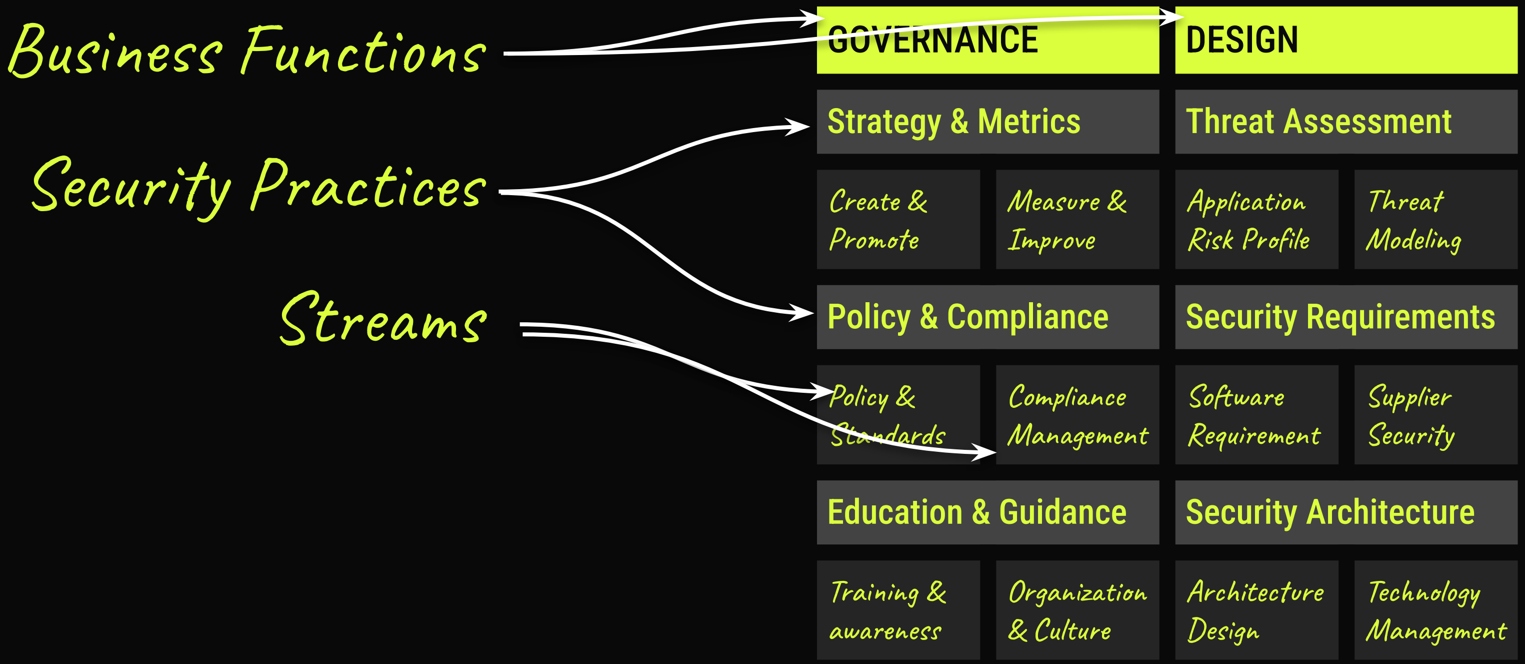


3 Assessment

The Model

GOVERNANCE		DESIGN		IMPLEMENTATION		VERIFICATION		OPERATIONS	
Strategy & Metrics		Threat Assessment		Secure Build		Arch. Assessment		Incident M.gement	
Create & Promote	Measure & Improve	Application Risk Profile	Threat Modeling	Build Process	Software Dependency	Architecture Validation	Architecture Mitigation	Incident Detection	Incident Response
Policy & Compliance		Security Requirements		Secure Deployment		Req.-driven Testing		Env. Management	
Policy & Standards	Compliance Management	Software Requirement	Supplier Security	Deployment Process	Secret Management	Control Verification	Mis-/abuse Testing	Config. Hardening	Patching & Updating
Education & Guidance		Security Architecture		Defect Management		Security Testing		Ops. Management	
Training & awareness	Organization & Culture	Architecture Design	Technology Management	Defect Tracking	Metrics & Feedback	Scalable Baseline	Deep Underst.ding	Data Protection	Decomm. & Legacy mng

The Model



Business Functions

Security Practices

Streams

GOVERNANCE		DESIGN	
Strategy & Metrics		Threat Assessment	
Create & Promote	Measure & Improve	Application Risk Profile	Threat Modeling
Policy & Compliance		Security Requirements	
Policy & Standards	Compliance Management	Software Requirement	Supplier Security
Education & Guidance		Security Architecture	
Training & awareness	Organization & Culture	Architecture Design	Technology Management

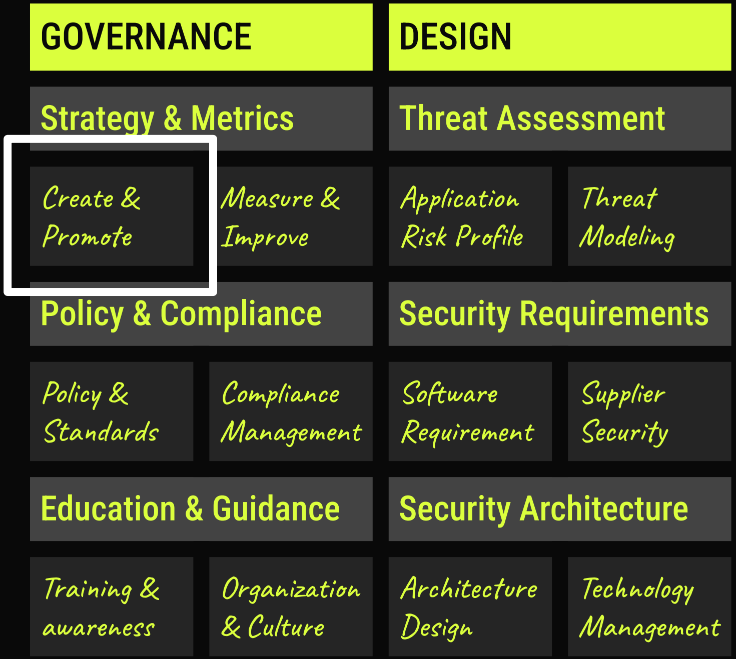
Maturity Level 1

Benefit

Common understanding of your organization's security posture

Activity

Common understanding of your organization's security posture, what threats exist or may exist, as well as how tolerant executive leadership is of these risks. This understanding is a key component of determining software security assurance priorities …



GOVERNANCE		DESIGN	
Strategy & Metrics		Threat Assessment	
Create & Promote	Measure & Improve	Application Risk Profile	Threat Modeling
Policy & Compliance		Security Requirements	
Policy & Standards	Compliance Management	Software Requirement	Supplier Security
Education & Guidance		Security Architecture	
Training & awareness	Organization & Culture	Architecture Design	Technology Management

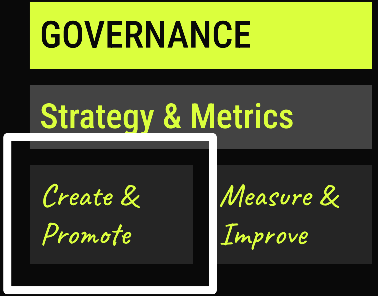
Maturity Level 1

Question

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

Quality criteria

- □ 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



*Assess one **scope** at a time!*

Maturity Level 1

Answers

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

GOVERNANCE

Strategy & Metrics

Create & Promote

Measure & Improve

Stream Guidance

SAMM team guidance Google Doc 🔗

Community guidance Google Doc 🔗

THE INTERVIEW

- Trust
- Style
- Premises
- Notes

4 Roadmap

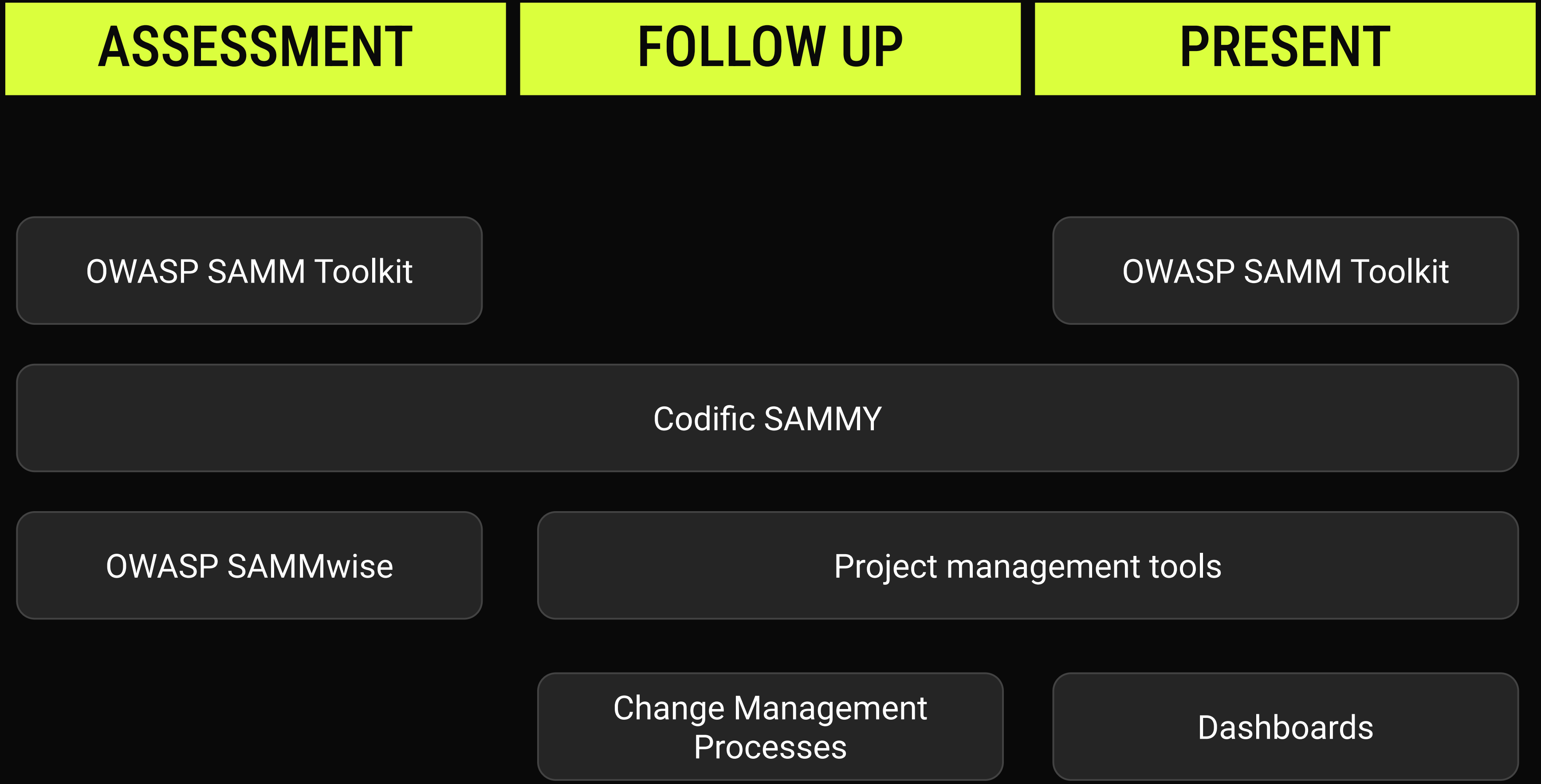
Roadmap

SAMM Roadmap vs Existing objectives

Existing change management process or yet another PM tool?

5

Tools & Processes



<table>
<tr><th>ASSESSMENT</th><th>FOLLOW UP</th><th>PRESENT</th></tr>
<tr><td>OWASP SAMM Toolkit</td><td></td><td>OWASP SAMM Toolkit</td></tr>
<tr><td colspan="3">Codific SAMMY</td></tr>
<tr><td>OWASP SAMMwise</td><td colspan="2">Project management tools</td></tr>
<tr><td></td><td>Change Management Processes</td><td>Dashboards</td></tr>
</table>

6 Culture

Resources

- owaspsamm.org
  - SAMM Team Guidance
  - Community Guidance
- meetup.com/owasp-samm
- youtube.com/@owaspsamm
- codific.com/the-owasp-samm-training
- Local OWASP Chapter events

- The person on your right
- (left, in front and behind too)

Thank you!

Questions & Answers