
SBA
Research

Secure Software Development

A short introduction of the OWASP SAMM

Michael Koppmann, SBA Research

B2B Software Days, May 08–10, 2023

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

FFG
Forschung wirkt.

wirtschafts agentur wien
Ein Fonds der Stadt Wien

European Commission

FWF
Der Wissenschaftsfonds.

netidee
OPEN INNOVATIONS

Who Am I?

- IT Security Consultant at SBA Research
  - Web application security
  - Spear phishing simulations
  - Source code audits
  - Architecture reviews
  - SAMM assessments
- Co-founder of the sec4dev conference

powered by:

SBA Research

sec4dev

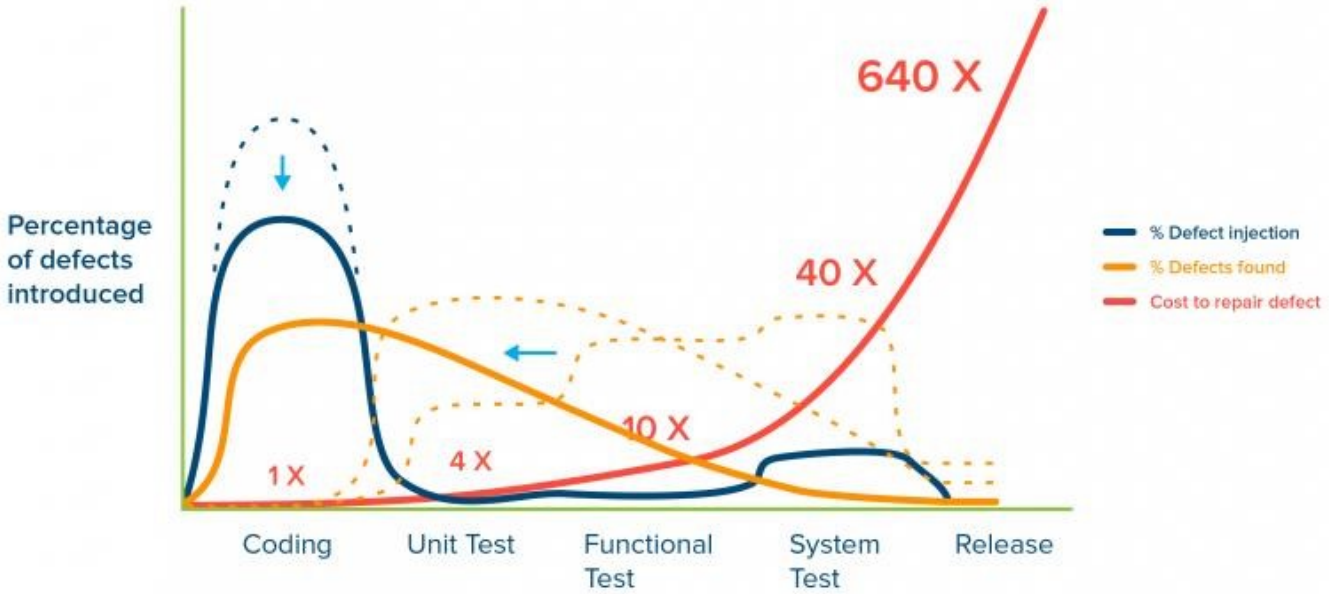
https://sec4dev.io

When you are a hands-on guy and start consulting

SECURE DEVELOPMENT LIFECYLE AUDITS

WEBAPP PENTEST

Shift Left



Jones, Capers. *Applied Software Measurement: Global Analysis of Productivity and Quality.*

Secure Development is not just Secure Coding

Example 1: Vulnerability in library

1. Undefined responsibilities between Dev & Ops
2. Missing automation
3. Software dependencies are not checked during build or deployment
4. A known vulnerability in a 3rd party library goes unnoticed
5. Internet-facing application gets exploited

Secure Development is not just Secure Coding

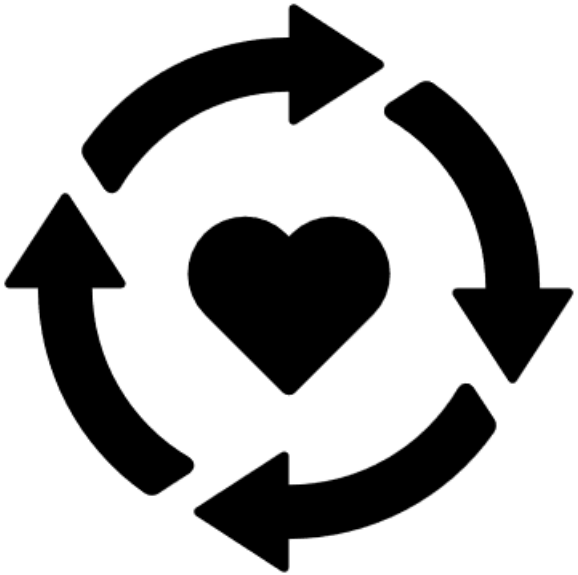
Example 2: Vulnerability found too late

1. No Threat Modeling or security architecture review done in advance
2. No security requirements in application design, only functional requirements
3. Penetration Test done at the end finds severe security vulnerabilities
4. Only two ways forward
    1. Security problems ignored, application goes live in an exploitable state
    2. Go back to design phase and update implementation; very expensive at this stage of the project


CHALLENGE ACCEPTED
imgflip.com

What Is A Secure Development Process?

- Considering security earlier
- Multi-layer security - Building strong safety nets
- Empowering developers
- Measuring and improving security
- Traceability of security decisions



OWASP SAMM

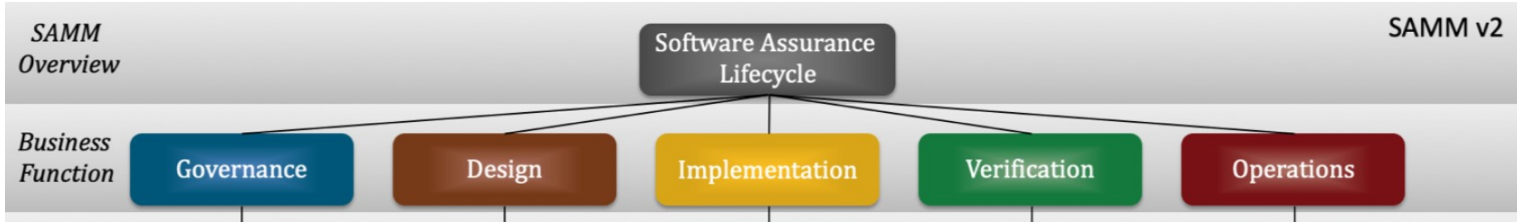
The model and the assessment

OWASP SAMM

- **What is it?**
  - Concise set of interview questions across security domains
  - Granular score in all areas
  - Proposals & activities how you can improve

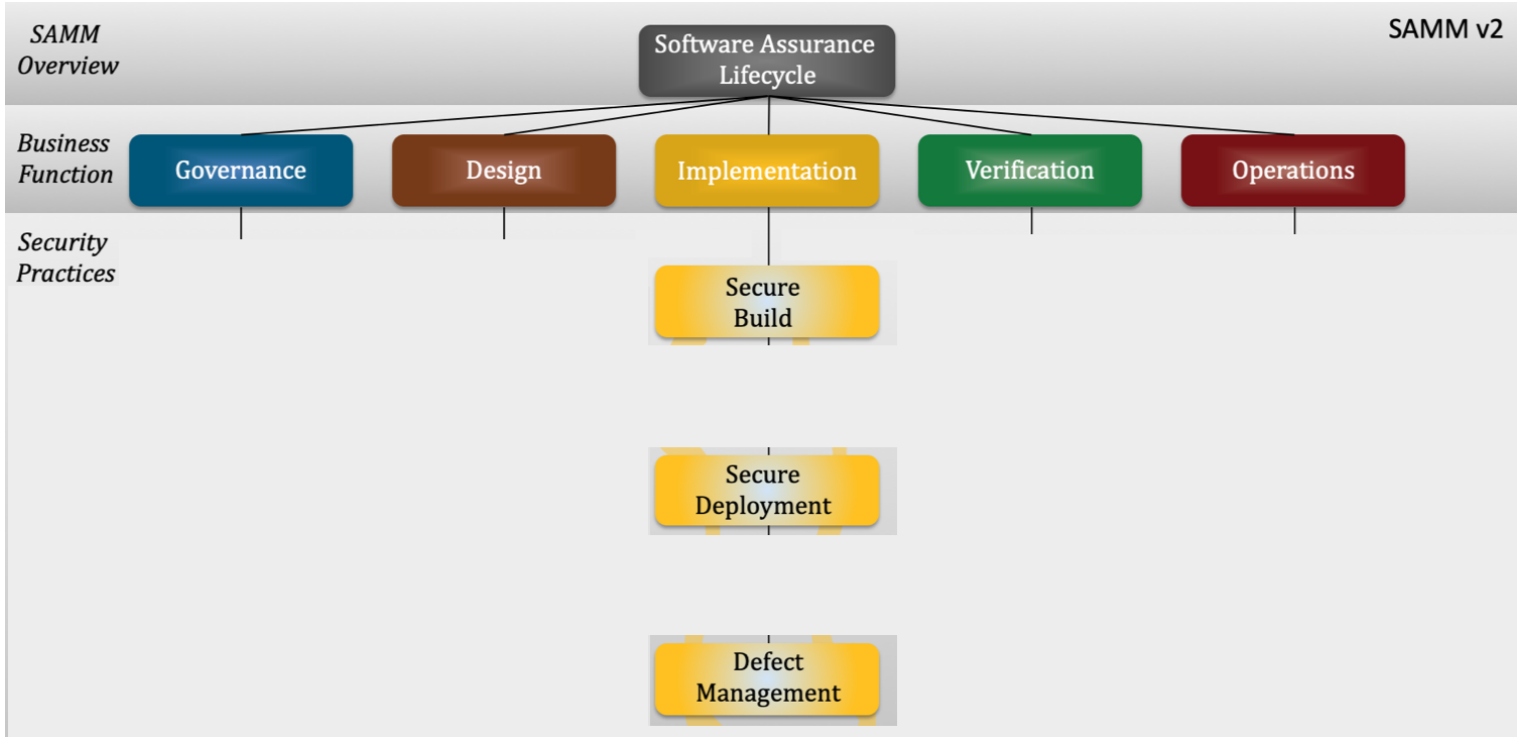
You talk to a team, SAMM tells you what to talk about.

OWASP SAMM
Business functions



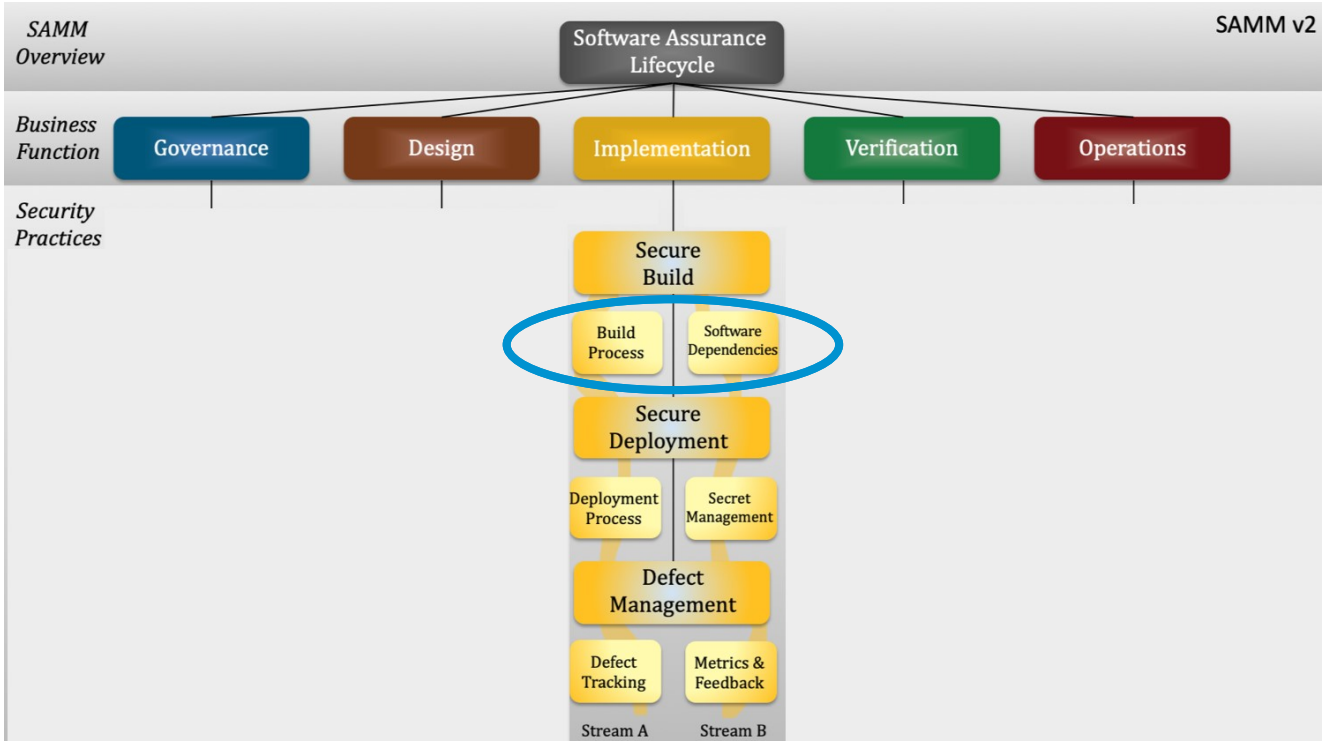
OWASP SAMM

Security practices



OWASP SAMM

Stream / activity



OWASP SAMM
Maturity level

Maturity level		Stream A Build Process	Stream B Software Dependencies
1	Build process is repeatable and consistent.	Create a formal definition of the build process so that it becomes consistent and repeatable.	Create records with Bill of Materials of your applications and opportunistically analyze these.
2	Build process is optimized and fully integrated into the workflow.	Automate your build pipeline and secure the used tooling. Add security checks in the build pipeline.	Evaluate used dependencies and ensure timely reaction to situations posing risk to your applications.
3	Build process helps prevent known defects from entering the production environment.	Define mandatory security checks in the build process and ensure that building non-compliant artifacts fails.	Analyze used dependencies for security issues in a comparable way to your own code.

https://owaspsamm.org/model/

OWASP SAMM

Activities

Model | Implementation | Secure Build | Build Process

MATURITY LEVEL 1 | MATURITY LEVEL 2 | MATURITY LEVEL 3

Benefit

Limited risk of human error during build process minimizing security issues

Activity

Define the build process, breaking it down into a set of clear instructions to either be followed by a person or an automated tool. The build process definition describes the whole process end-to-end so that the person or tool can follow it consistently each time and produce the same result. The definition is stored centrally and accessible to any tools or people. Avoid storing multiple copies as they may become unaligned and outdated.

The process definition does not include any secrets (specifically considering those needed during the build process).

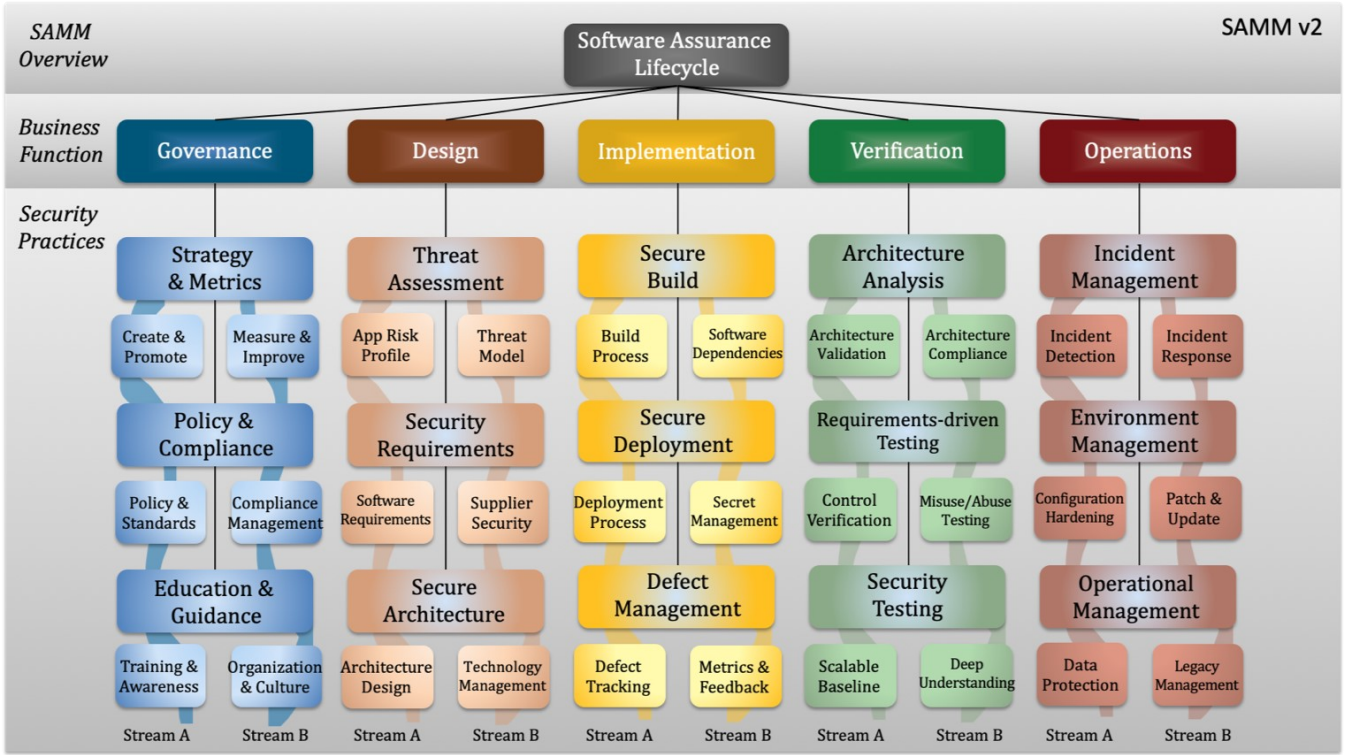
Review any build tools, ensuring that they are actively maintained by vendors and up-to-date with security patches. Harden each tool's configuration so that it is aligned with vendor guidelines and industry best practices.

Determine a value for each generated artifact that can be later used to verify its integrity, such as a signature or a hash. Protect this value and, if the artifact is signed, the private signing certificate.

Ensure that build tools are routinely patched and properly hardened.

https://owaspsamm.org/model/implementation/secure-build/stream-a/

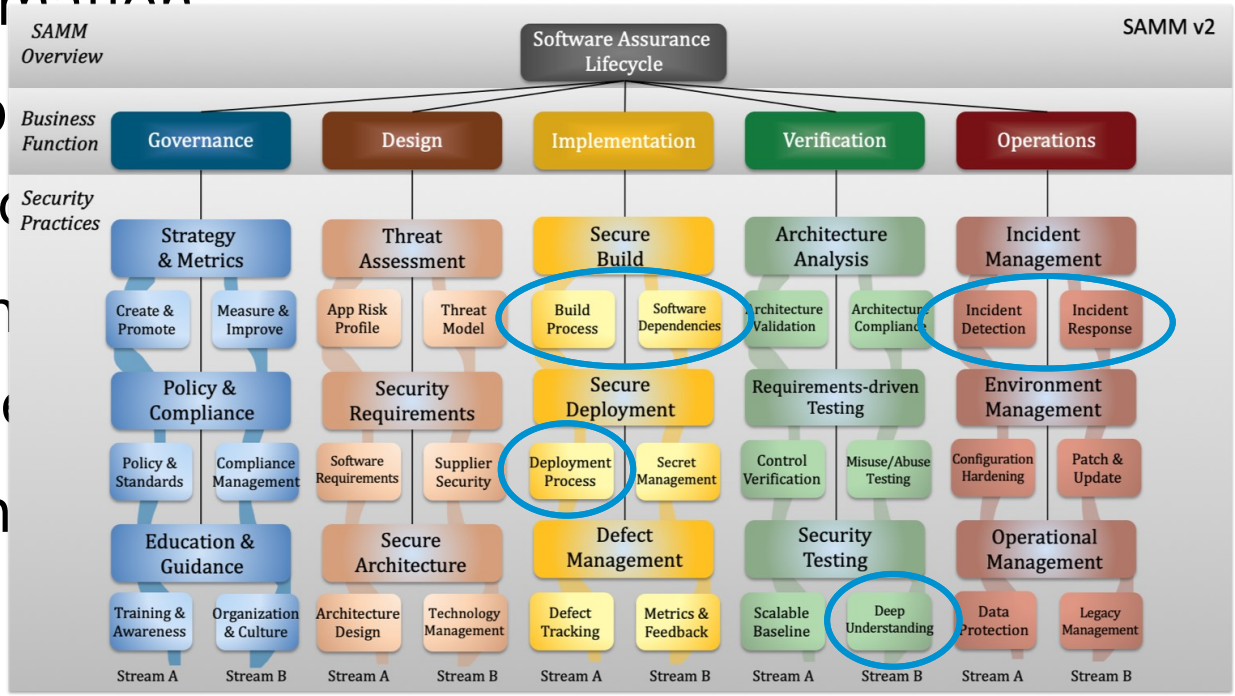
OWASP SAMM
Overview



Secure Development is not just Secure Coding

Example 1, revisited

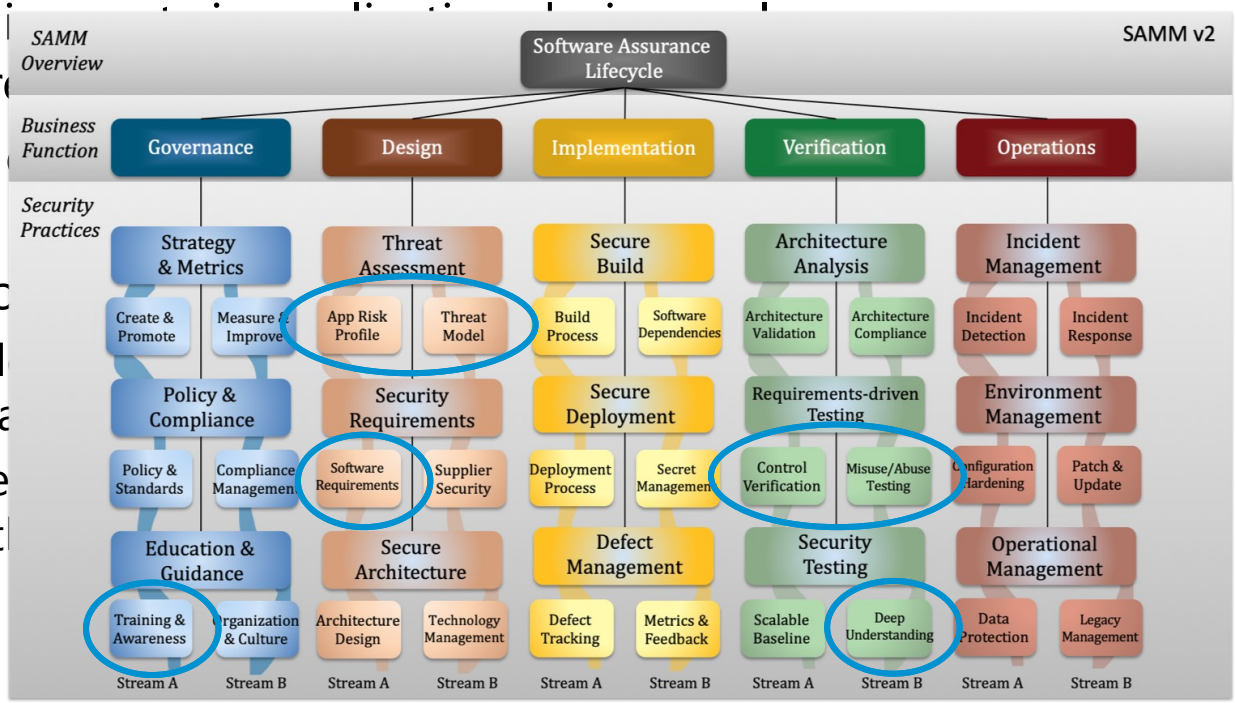
1. Undefined responsibilities between Dev & Ops
2. Missing automation
3. Software dep
   build or deplo
4. A known vuln
   goes unnotic
5. Internet-facin



Secure Development is not just Secure Coding

Example 2, revisited

1. No Threat Modeling or security architecture review done in advance
2. No security requi
   functional requir
3. Penetration Test
   vulnerability
4. Only two ways fc
   1. Security probl
      exploitable sta
   2. Go back to de
      expensive at t



Output & Results
Scoring

- **What you get**
  - A scored result for each function
  - Every activity has the same weight
  - Every level has the same weight
  - Helps detect blind spots
- **What you don't get**
  - Overall score

		Current Maturity Score			
			Maturity		
Functions	Security Practices	Current	1	2	3
Governance	Strategy & Metrics	0,63	0,25	0,25	0,13
Governance	Policy & Compliance	0,63	0,50	0,13	0,00
Governance	Education & Guidance	0,75	0,38	0,13	0,25
Design	Threat Assessment	0,50	0,25	0,25	0,00
Design	Security Requirements	0,25	0,25	0,00	0,00
Design	Secure Architecture	0,88	0,50	0,13	0,25
Implementation	Secure Build	1,88	1,00	0,63	0,25
Implementation	Secure Deployment	1,13	0,75	0,38	0,00
Implementation	Defect Management	0,63	0,63	0,00	0,00
Verification	Architecture Assessment	0,88	0,75	0,00	0,13
Verification	Requirements Testing	0,75	0,25	0,25	0,25
Verification	Security Testing	1,50	0,75	0,50	0,25
Operations	Incident Management	0,13	0,13	0,00	0,00
Operations	Environment Management	0,50	0,38	0,13	0,00
Operations	Operational Management	1,25	1,00	0,13	0,13

Output & Results
Roadmap

- **Main output of assessment**
  - Status quo
  - Motivation and goals for short-term and long-term development
- **Where should I start?**
  - Ways to improve optimally and easiest
  - Activities that are almost established already
  - Most relevant activities in the given environment

Interviews

How assessments are done

Assessment Types

- **External interviewers**
  - Security experts are interviewers
  - Report with suggestions for moving forward
- **Self assessment**
  - Interview done by the team itself
  - Much faster since no evidence is collected
  - Can be done more often

Interview

- 1-5 team members with different roles get interviewed
- 2 interviewers
- Preparation
  - Interviewers should know about team, organization & software
  - Teams should have relevant documents and software at hand
- Initially takes ~1 day to interview a team

Questionnaire
Questions

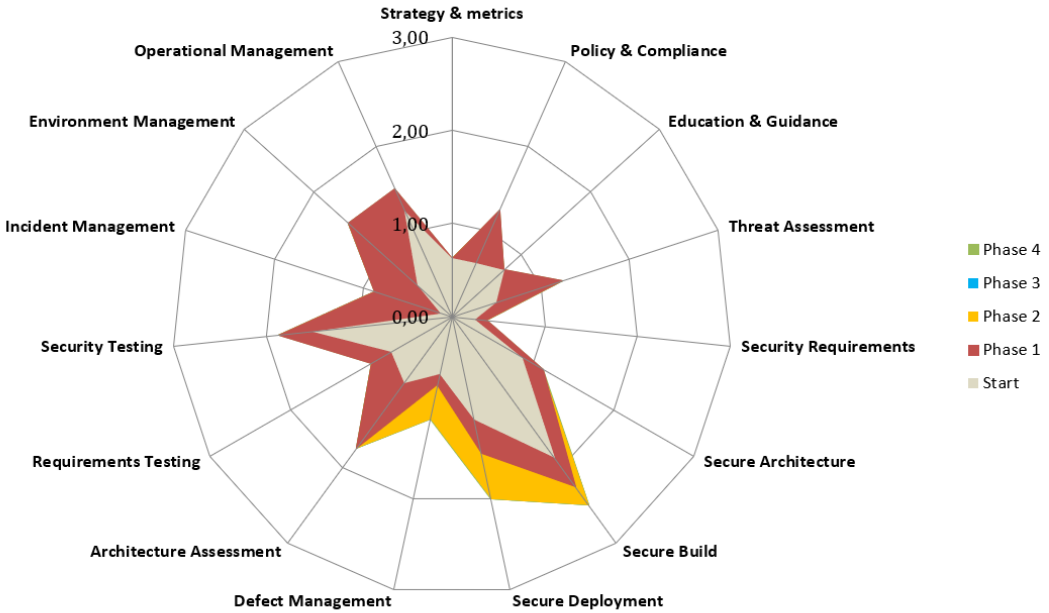
Compliance Management	**1**	**Do you have a complete picture of your external compliance obligations?**	**Yes, for at least half of the applications**	GDPR (DVR registration available but not well known in team, data changes are reported to Data Protection Officer)
		You have identified all sources of external compliance obligations You have captured and reconciled compliance obligations from all sources		ISO-27001 certification should come soon Customer NDAs available and known to the team
	2	**Do you have a standard set of security requirements and verification procedures addressing the organization's external compliance obligations?**	**No**	No checks
		You map each external compliance obligation to a well-defined set of application requirements You define verification procedures, including automated tests, to verify compliance with compliance-related requirements		
	3	**Do you regularly report on adherence to external compliance obligations and use that information to guide efforts to close compliance gaps?**	**No**	
		You have established, well-defined compliance metrics You measure and report on applications' compliance metrics regularly Stakeholders use the reported compliance status information to identify compliance gaps and prioritize gap remediation efforts		No

Questionnaire

Roadmap

Implementation			Current		Phase I	
Stream	Level	Secure Build	Answer	Rating	Answer	Rating
Build Process	1	Is your full build process formally described?	Yes, for most or all of the applications	1,88	Yes, for most or all of the applications	2,25
	2	Is the build process fully automated?	Yes, for most or all of the applications		Yes, for most or all of the applications	
	3	Do you enforce automated security checks in your build processes?	Yes, for some applications		Yes, for at least half of the applications	
Software Dependencies	1	Do you have solid knowledge about dependencies you're relying on?	Yes, for most or all of the applications		Yes, for most or all of the applications	
	2	Do you handle 3rd party dependency risk by a formal process?	Yes, for some applications		Yes, for at least half of the applications	
	3	Do you prevent build of software if it's affected by vulnerabilities in dependencies?	Yes, for some applications		Yes, for at least half of the applications	
Stream	Level	Secure Deployment	Answer	Rating	Answer	Rating
Deployment Process	1	Do you use repeatable deployment processes?	Yes, for most or all of the applications	1,13	Yes, for most or all of the applications	1,50
	2	Are deployment processes automated and employing security checks?	Yes, for some applications		Yes, for at least half of the applications	
	3	Do you consistently validate the integrity of deployed artifacts?	No		No	
Secret Management	1	Do you limit access to application secrets according to the least privilege principle?	Yes, for at least half of the applications		Yes, for most or all of the applications	
	2	Do you inject production secrets into configuration files during deployment?	Yes, for at least half of the applications		Yes, for at least half of the applications	
	3	Do you practice proper lifecycle management for application secrets?	No		No	
Stream	Level	Defect Management	Answer	Rating	Answer	Rating
Defect Tracking	1	Do you track all known security defects in accessible locations?	Yes, for most or all of the applications	0,63	Yes, for most or all of the applications	0,75
	2	Do you keep an overview of the state of security defects across the organization?	No		Yes, for some applications	
	3	Do you enforce SLAs for fixing security defects?	0		0	
Metrics and Feedback	1	Do you use basic metrics about recorded security defects to carry out quick win improvement activities?	Yes, for some applications		Yes, for some applications	
	2	Do you improve your security assurance program upon standardized metrics?	No		No	
	3	Do you regularly evaluate the effectiveness of your security metrics so that its input helps drive your security strategy?	No		No	

Roadmap
Score graph



TL;DR

- Pick a project/team
- Choose 2 interviewers
- Use spreadsheet to conduct interview
  - Use OWASP SAMM website if you get lost
- Merge notes & scores
- Specify roadmap with easy wins & blind spots

Danielle MacInnes, https://unsplash.com/photos/IuLgi9PWETU

Michael Koppmann

SBA Research

Floragasse 7, 1040 Vienna

mkoppmann@sba-research.org

Matrix: @mkoppmann:sba-research.org

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

Bundesministerium Digitalisierung und Wirtschaftsstandort

FFG Forschung wirkt.

wirtschaftsagentur wien Ein Fonds der Stadt Wien

European Commission

FWF Der Wissenschaftsfonds.

netidee OPEN INNOVATIONS