SBA
Research

1.400 hours for the preparation of an ISO27001 certification within 15 minutes and the connex to an espresso.

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

Bundesministerium
Arbeit und Wirtschaft

FFG
Forschung wirkt.

wirtschafts
agentur
wien

Für die
Stadt Wien

European
Commission

FWF Österreichischer
Wissenschaftsfonds

netidee
FÖRDERUNGEN

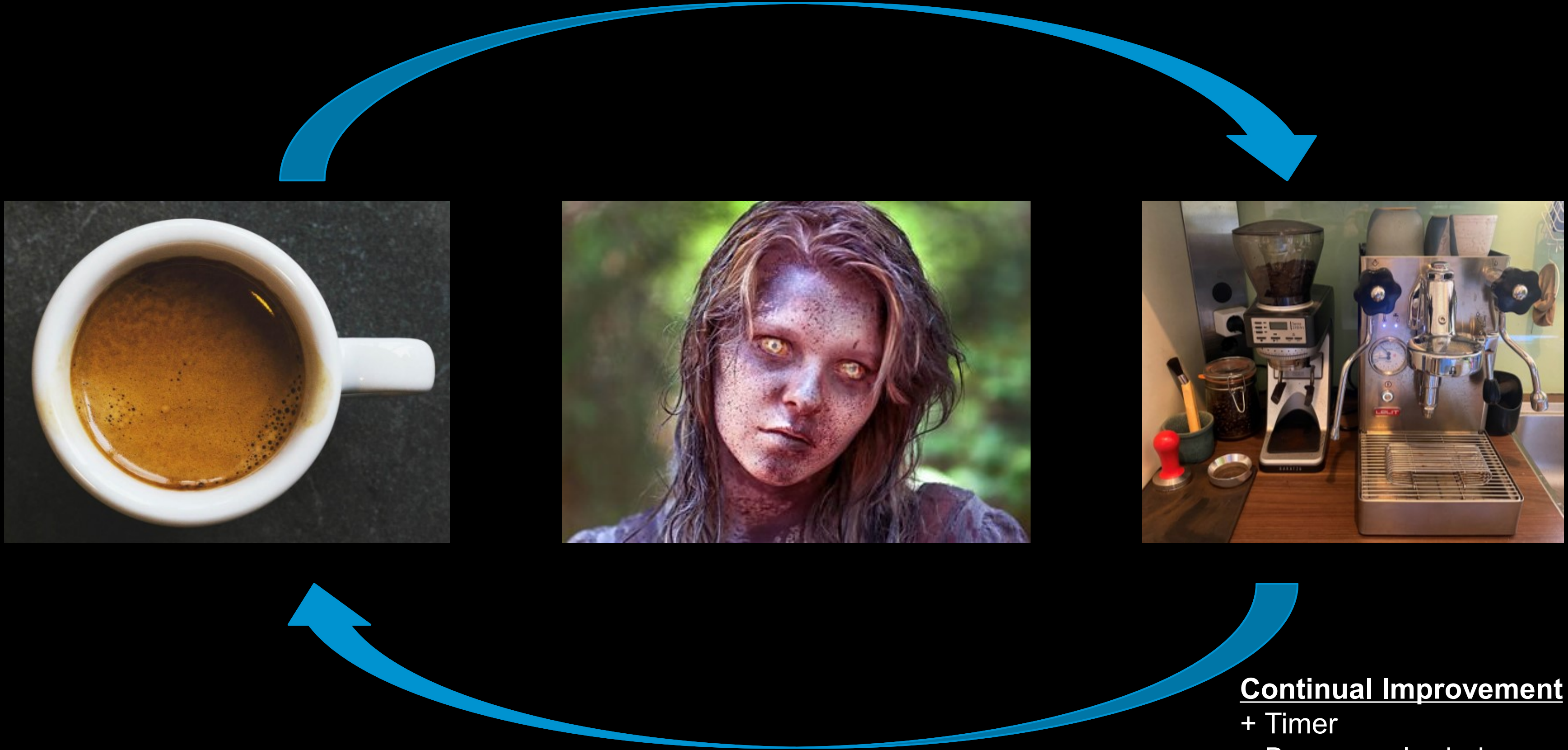
Please choose my cap ☺

- Since 17+ years in “the” InfoSec field (and SBA)
  - Main consulting **focus on security governance**
  - ISO27001 lead auditor and implementer, etc.

- **CISO** within the research center SBA Research
  - Research area (maybe NIS-2 challenge)
  - Professional Services = ISO27001 certified

- Prokurist = **responsible for business success**

For an ISO27001 certification you need an InformationSecurityManagementSystem (ISMS)



Continual Improvement

+ Timer

+ Bean supply chain

+ Adequate controls

… etc.

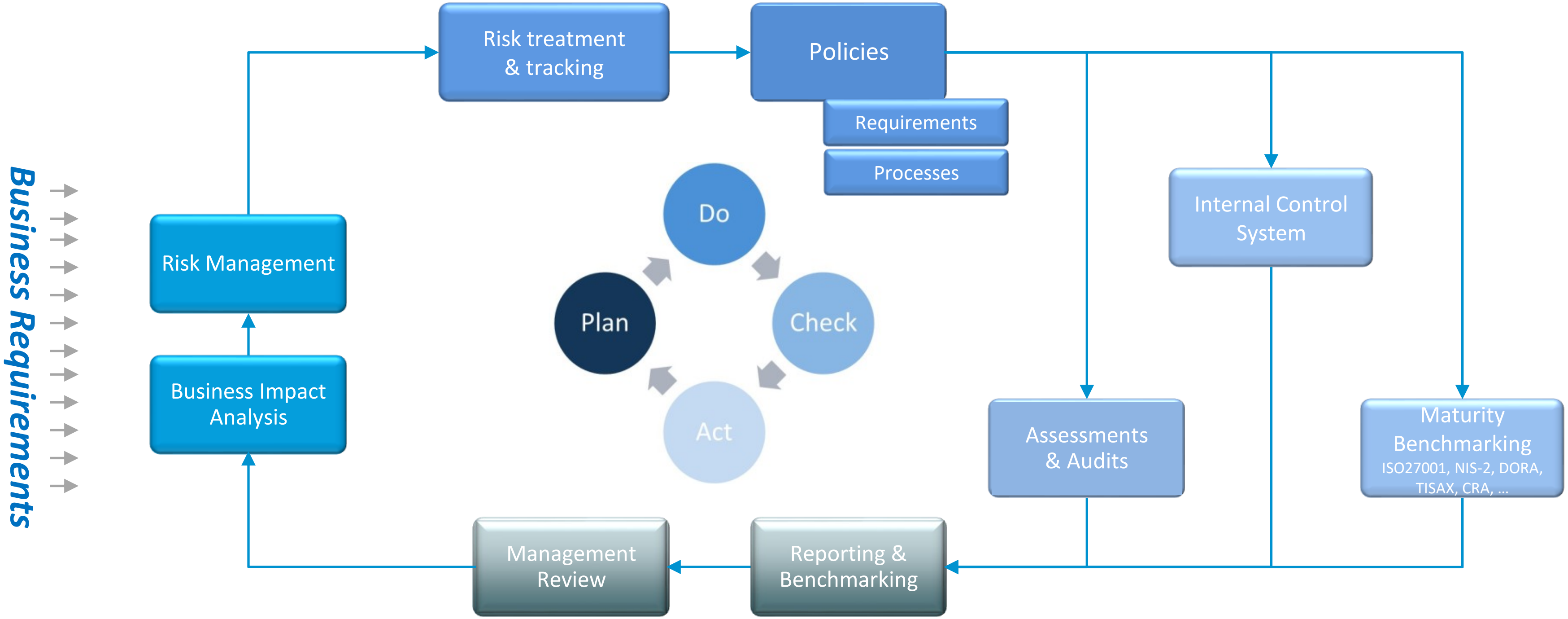
An ISMS...

… is a **systematic approach for** establishing, implementing, operating, monitoring, reviewing, maintaining and improving **an organization's information security to achieve business objectives**.

It is **based upon** a risk assessment and **the organization's risk acceptance levels** designed to effectively treat and manage risks.

Source: ISO27000

Schematic ISMS Cycle

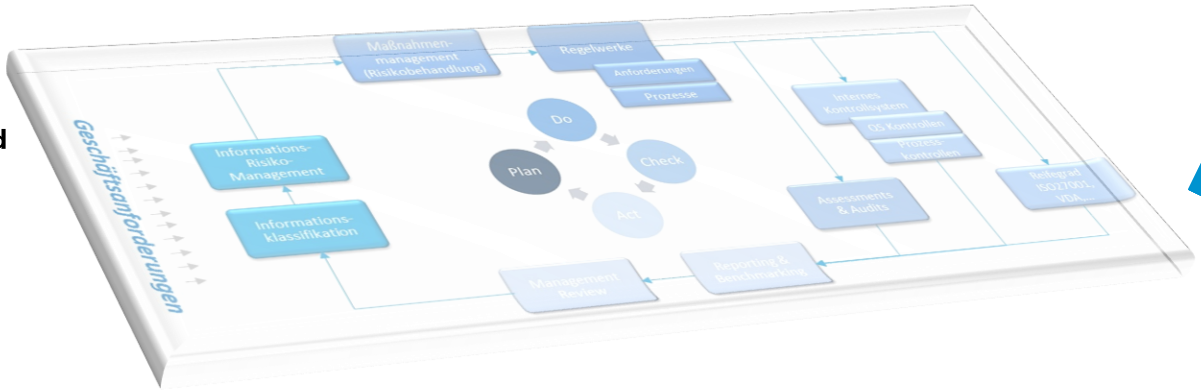


Why so expensive / time-consuming?

ISMS & Security Controls (Measures)

<u>Risk Management</u>
Ensure that no (new) risk remains untreated

- Risk analyses
- Polices
- Measures
- Trainings
- …



<u>Quality Assurance</u>
Indicators whether ISMS is effective

- GAP Analyses
- Technical audits
- Internal controls
- Accepted risks
- Security Incidents
- …

Employees	Applications	Clients	Network	…
Passwords	Secure access	Security updates	Firewall	
USB Sticks	Authorization	Malware protection	Segmentation	
Phishing	Secure code	Encryption	Attack detection	
…	…	…	…	
Secure working	*Secure Applications*	*Secure resources*	*Secure communication*	

Example: NIS-2 Risk Management Areas

(1) Management

(2) Security Polices

(3) Risk Management

(4) Asset Management

(5) HR security

(6) Awareness

(7) Supply Chain Security

(8) Access Management

(9) Procurement, development, operation and maintenance
(g) Software Security

(10) Cryptography

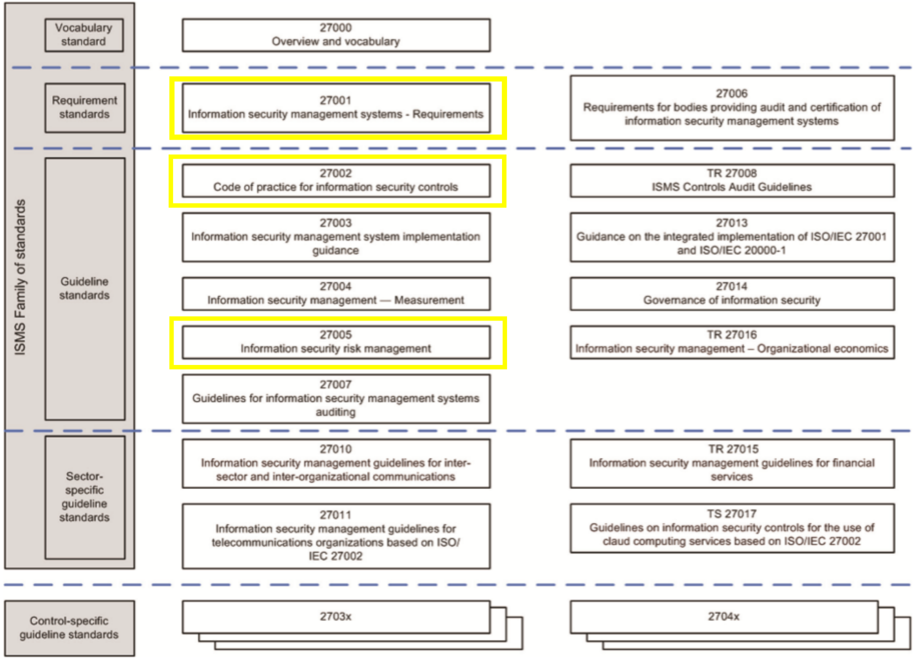
(11) Security Incident Mgmt

(12) Business Continuity and Crisis Management

(13) Physical Security

+/- 50 measures

Don’t reinvent the wheel!



ISMS Family of standards

Vocabulary standard

27000 Overview and vocabulary

Requirement standards

27001 Information security management systems - Requirements

27006 Requirements for bodies providing audit and certification of information security management systems

Guideline standards

27002 Code of practice for information security controls

TR 27008 ISMS Controls Audit Guidelines

27003 Information security management system implementation guidance

27013 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

27004 Information security management — Measurement

27014 Governance of information security

27005 Information security risk management

TR 27016 Information security management – Organizational economics

27007 Guidelines for information security management systems auditing

Sector-specific guideline standards

27010 Information security management guidelines for inter-sector and inter-organizational communications

TR 27015 Information security management guidelines for financial services

27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

TS 27017 Guidelines on information security controls for the use of claud computing services based on ISO/IEC 27002

Control-specific guideline standards

2703x

2704x

Figure 1 — ISMS Family of Standards Relationships

Supplementary ISO-Standards

- 27017 Cloud Services
- 27034 Application Security
- 22301 Business Continuity

Supplementary Best-Practices

- BSI Grundschutzkompendium
- CIS CSC & Benchmarks
- OWASP Top10, ASVS, SAMM, etc.
- CSA Cloud Security
- NIST CSF
- …

The Why?

BEPPO MUSS EIN BISSCHEN LACHEN, ALS IHM DIE UNSINNIGKEIT SEINER TAT BEWUSST WIRD.
WWW.NICHTLUSTIG.DE

Business Case vs Business Risks

- ISO27001 certification required in order to secure revenue streams, e.g.
  - … be chosen as **trusted** security service partner
  - … be able to participate in **tenders**
  - … be able to provide comprehensible **proof**
    - Established information security processes.
    - Security of clients' confidential data (e.g. critical exploitable vulnerabilities)
  - … be an NISG **qualified body** (QuaSte)
  - (… NIS-2 **regulatory compliance**)

Business Case vs Business Risks

1. **Breach of contract**, e.g. non-compliance with a confidentiality agreement
2. (Negligent) **damage to a customer**, e.g. due to security tests
3. Lasting **damage to reputation**, e.g. due to negligent misconduct (data leakage)

>> Defines our **business case for information security** (= risk appetite & security posture)

ISMS effort

Less effort if…

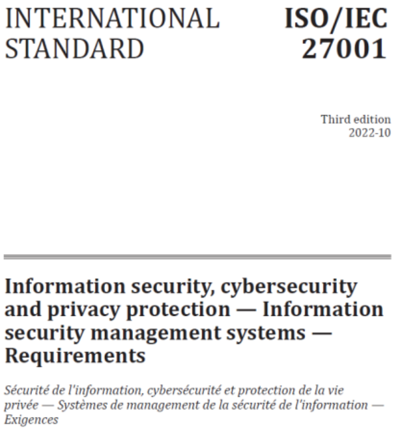
- Clear business case
- Small org. structure
- High homogeneity

More effort if…

- Large org. structure
- Low homogeneity
- Regulatory pressure

If your focus lies on software (products)

… think about a management system for application security



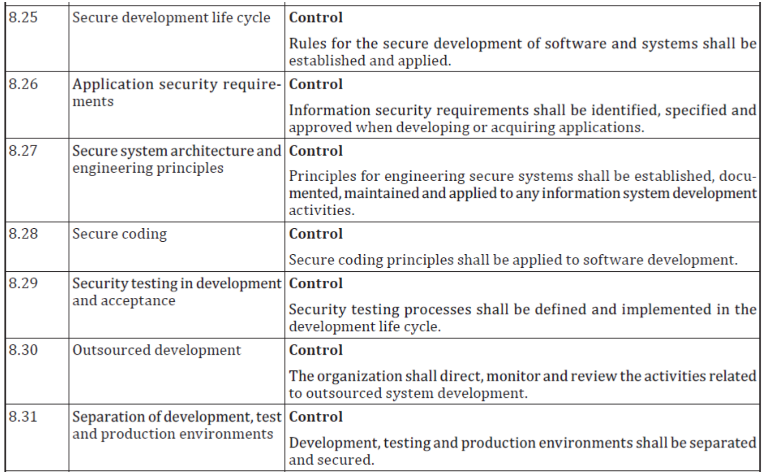
INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

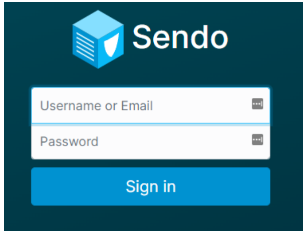


8.25	Secure development life cycle	**Control** Rules for the secure development of software and systems shall be established and applied.
8.26	Application security requirements	**Control** Information security requirements shall be identified, specified and approved when developing or acquiring applications.
8.27	Secure system architecture and engineering principles	**Control** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.
8.28	Secure coding	**Control** Secure coding principles shall be applied to software development.
8.29	Security testing in development and acceptance	**Control** Security testing processes shall be defined and implemented in the development life cycle.
8.30	Outsourced development	**Control** The organization shall direct, monitor and review the activities related to outsourced system development.
8.31	Separation of development, test and production environments	**Control** Development, testing and production environments shall be separated and secured.

Source: ISO/IEC 27002:2022

OWASP SAMM

Software Assurance Maturity Model



Referenced Standards & Frameworks

ISMS Information Security Management System

- ISO Standards ::Link::
- BSI Grundschutz ::Link::

Cyber Defense

- CIS CSC & Benchmarks ::Link::
- NIST CSF ::Link::

Software Security & Maturity

- OWASP SAMM ::Link::
- OWASP ASVS ::Link::

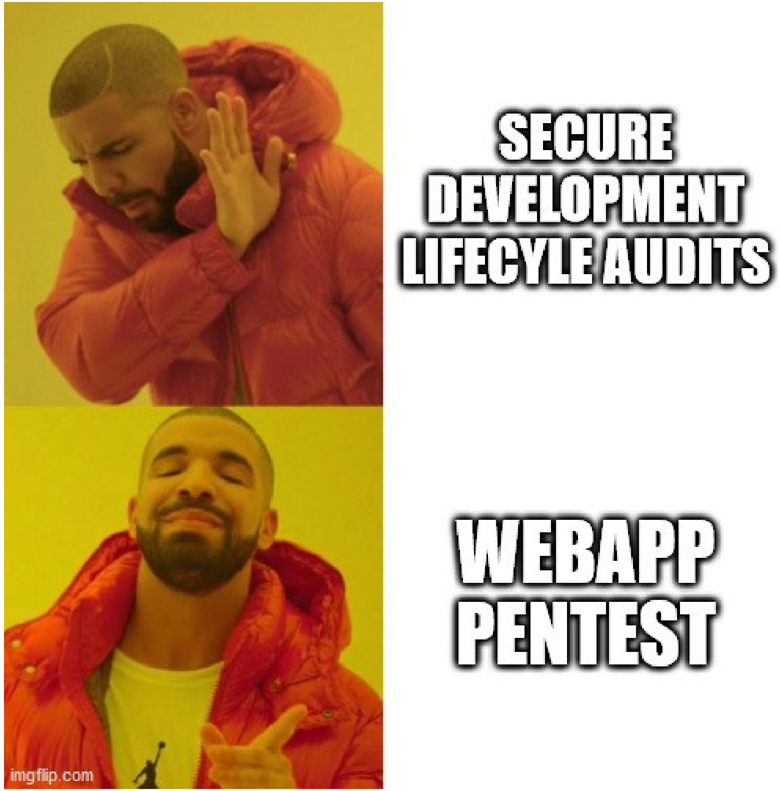
Secure Software Development

A Short Introduction to the OWASP SAMM

Who Am I?

- IT Security Consultant at SBA Research
  - Web application security
  - Spear phishing simulations
  - Source code audits
  - Architecture reviews
  - SAMM assessments
  - Security training
- Software developer

When you are a hands-on guy and start consulting



Secure Development is not just Secure Coding

Example: 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

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

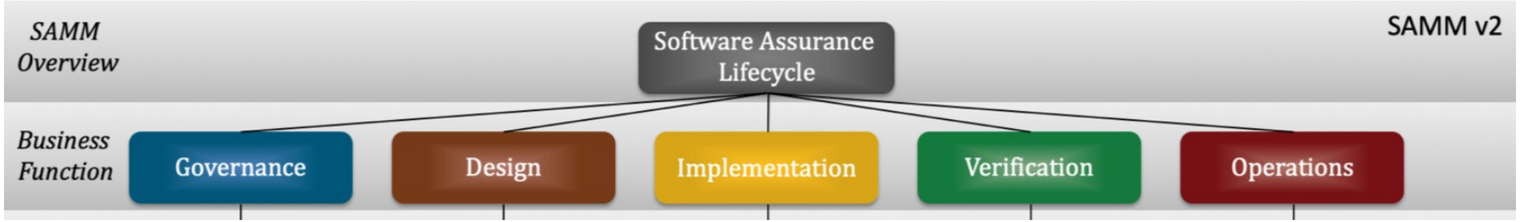
OWASP SAMM

- **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.

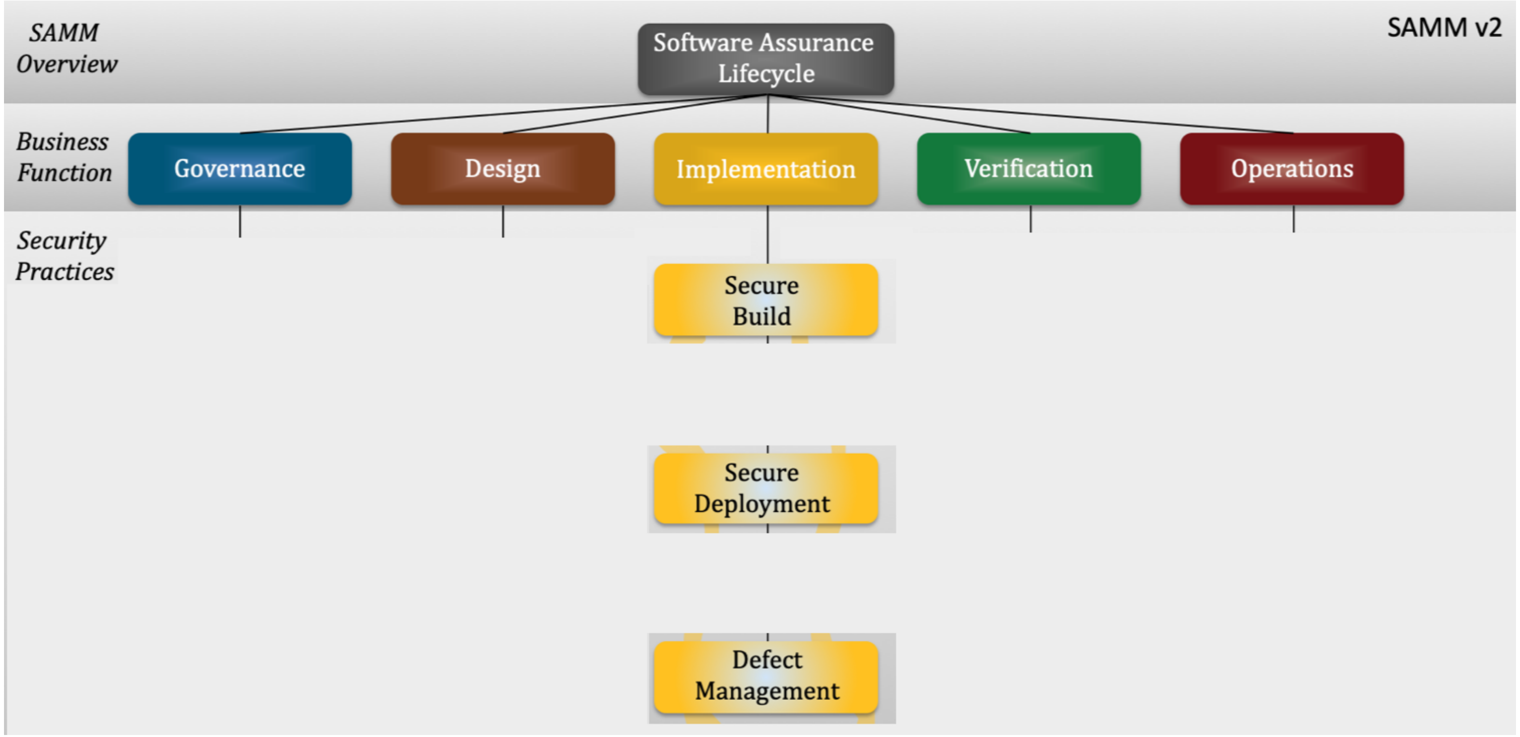
OWASP SAMM

Business functions



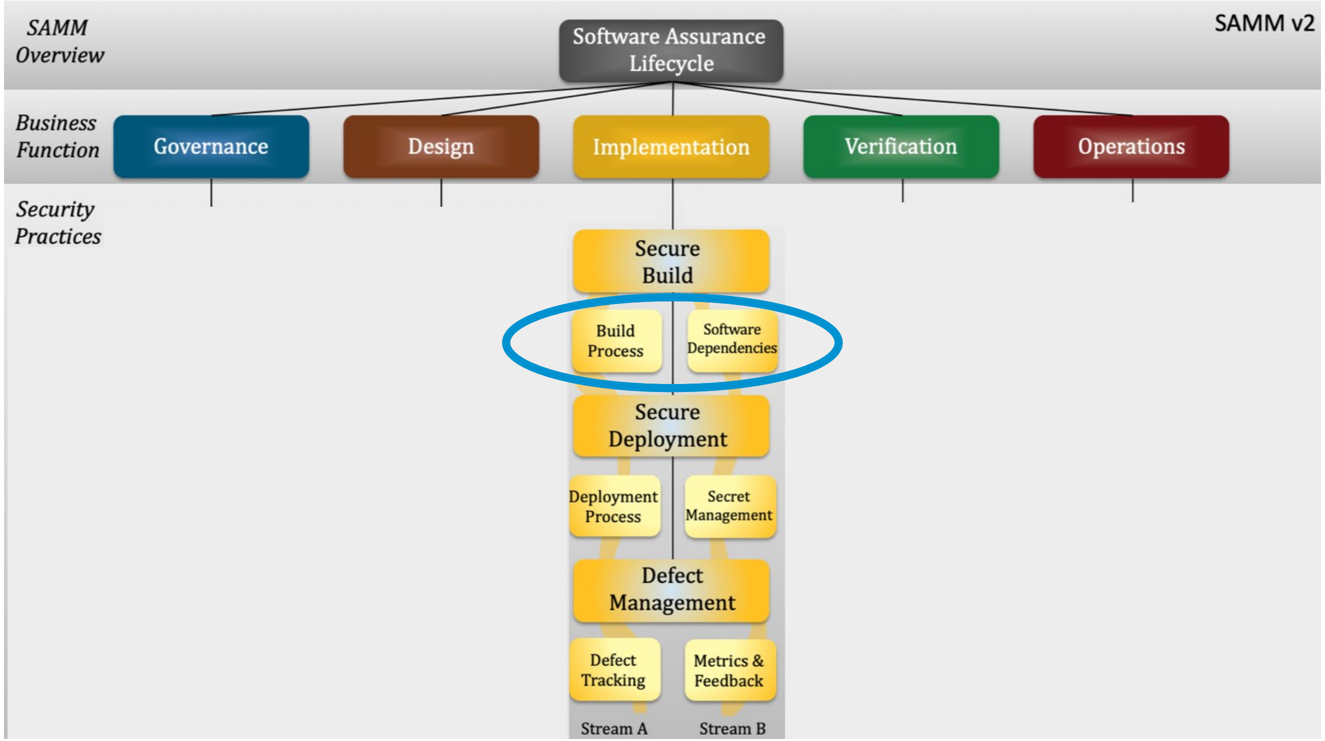
OWASP SAMM

Security practices



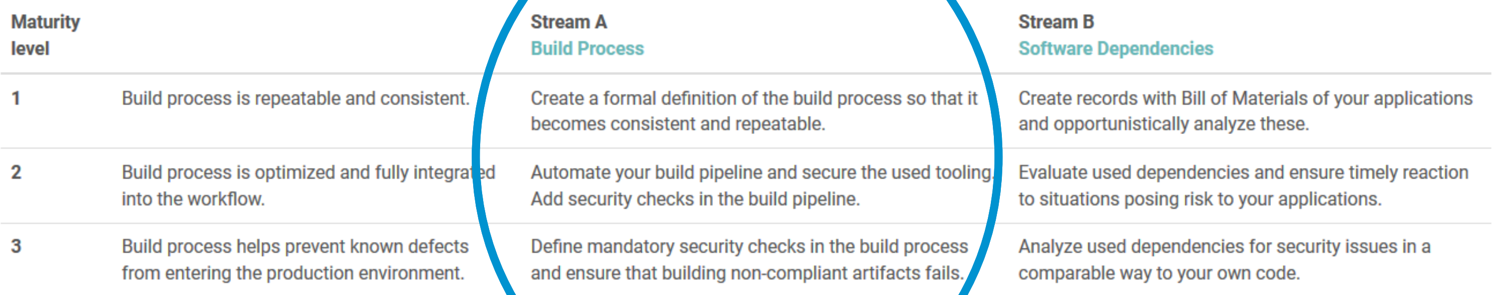
OWASP SAMM

Stream / activity



OWASP SAMM

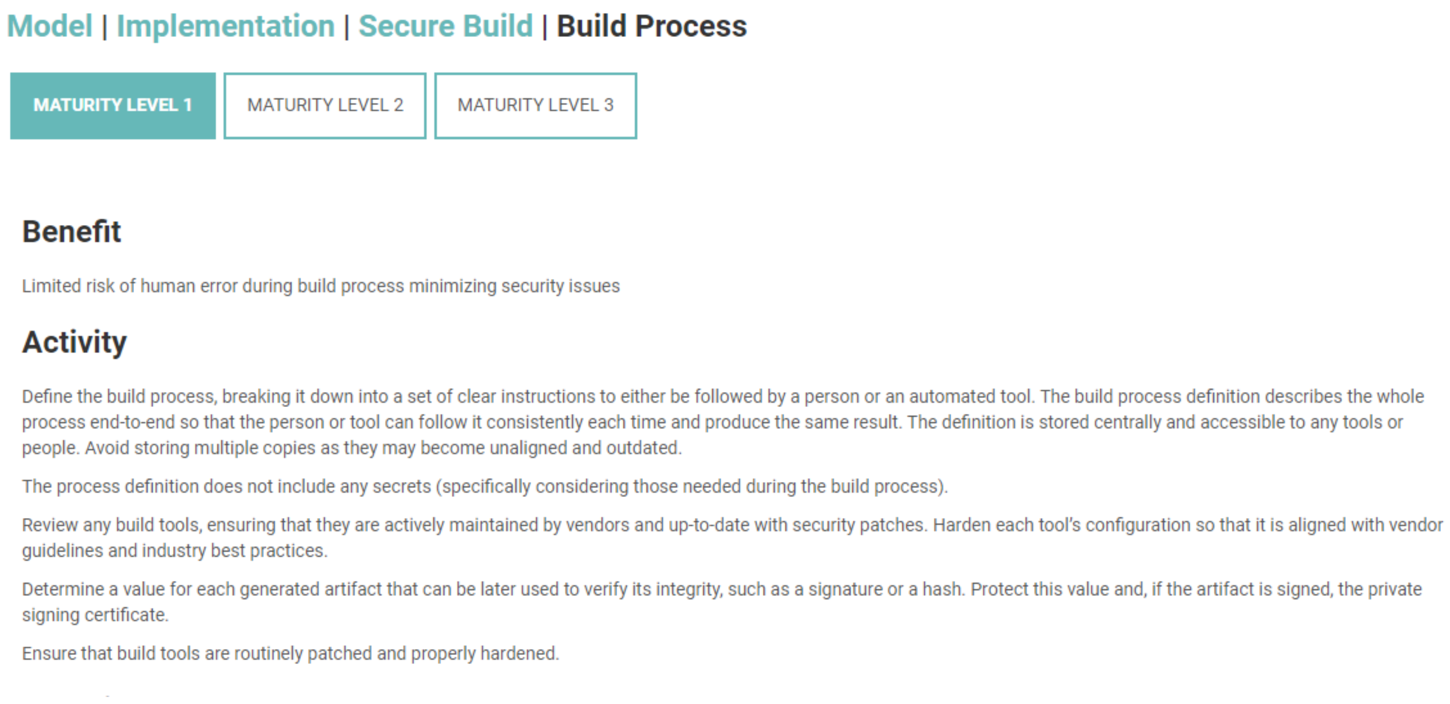
Maturity level



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

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.

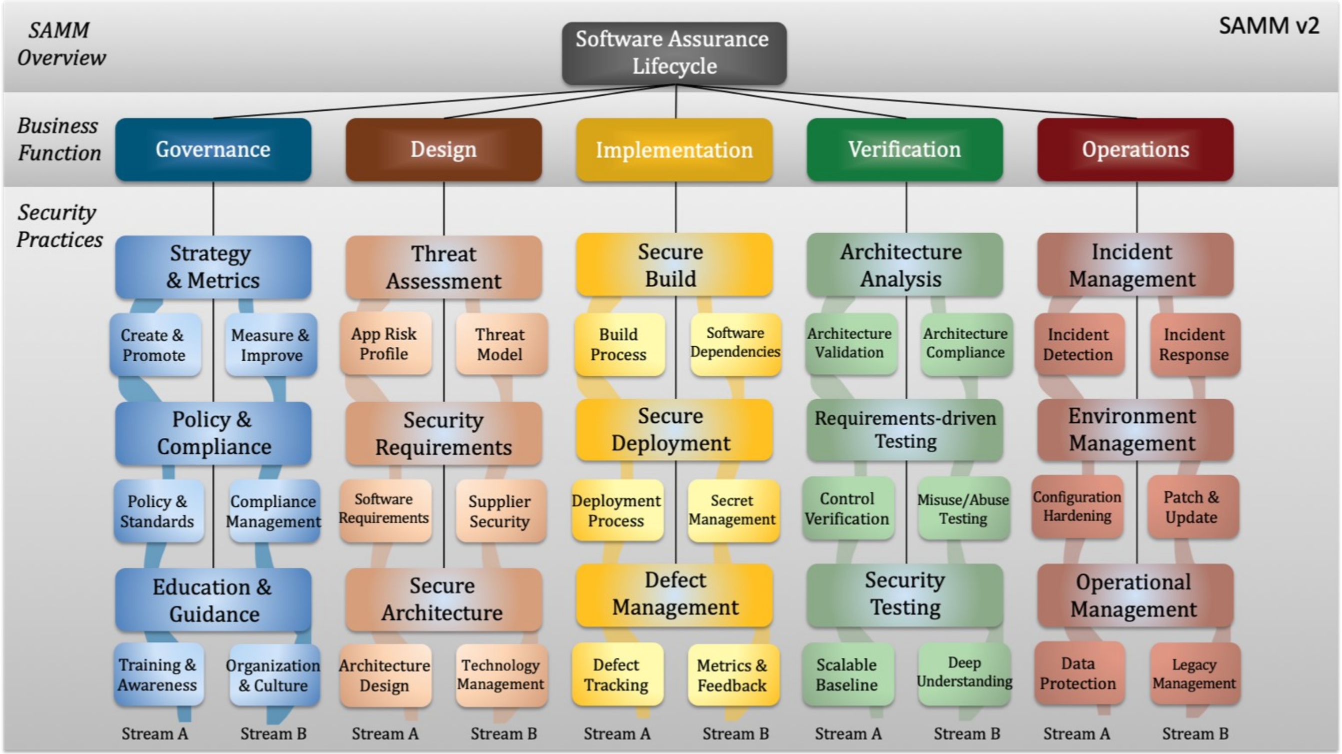
Determine a value for each generated artifact that can be later used to verify its integrity, such as a signature or a hash. Protect this value and, if the artifact is signed, the private signing certificate.

Ensure that build tools are routinely patched and properly hardened.

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

OWASP SAMM

Overview



SAMM Overview

SAMM v2

Software Assurance Lifecycle

Business Function

Security Practices

Governance
- Strategy & Metrics: Create & Promote; Measure & Improve
- Policy & Compliance: Policy & Standards; Compliance Management
- Education & Guidance: Training & Awareness; Organization & Culture

Design
- Threat Assessment: App Risk Profile; Threat Model
- Security Requirements: Software Requirements; Supplier Security
- Secure Architecture: Architecture Design; Technology Management

Implementation
- Secure Build: Build Process; Software Dependencies
- Secure Deployment: Deployment Process; Secret Management
- Defect Management: Defect Tracking; Metrics & Feedback

Verification
- Architecture Analysis: Architecture Validation; Architecture Compliance
- Requirements-driven Testing: Control Verification; Misuse/Abuse Testing
- Security Testing: Scalable Baseline; Deep Understanding

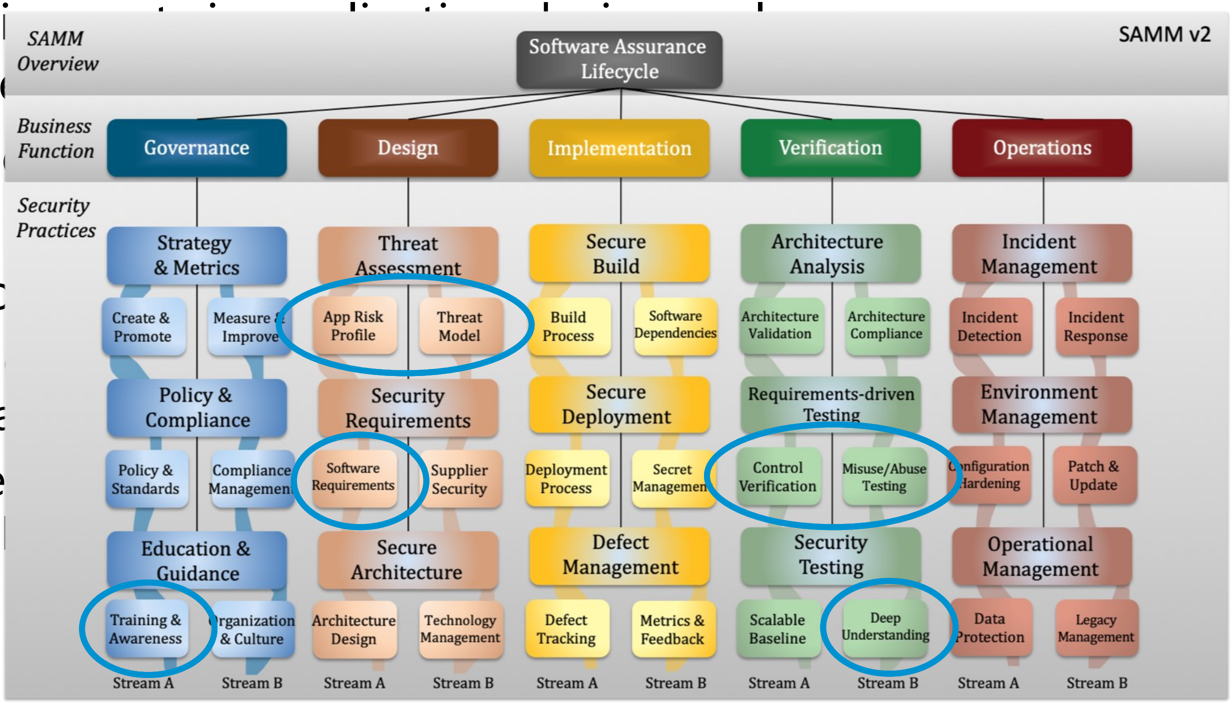
Operations
- Incident Management: Incident Detection; Incident Response
- Environment Management: Configuration Hardening; Patch & Update
- Operational Management: Data Protection; Legacy Management

Stream A Stream B Stream A Stream B Stream A Stream B Stream A Stream B Stream A Stream B

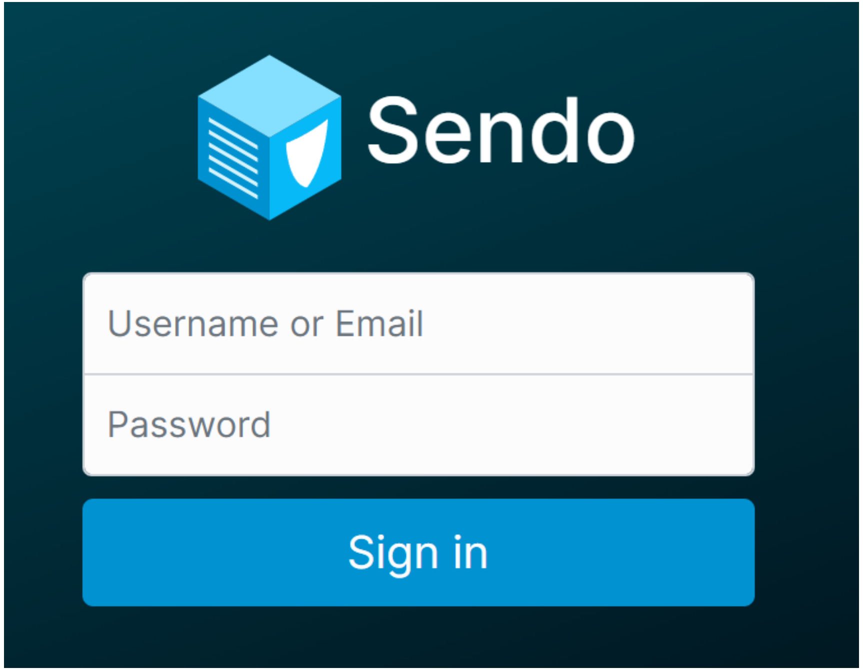
Secure Development is not just Secure Coding

Example, 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 fo
   1. Security probl exploitable sta
   2. Go back to de expensive at t



OWASP SAMM At SBA



Sendo

Username or Email

Password

Sign in

OWASP SAMM At SBA

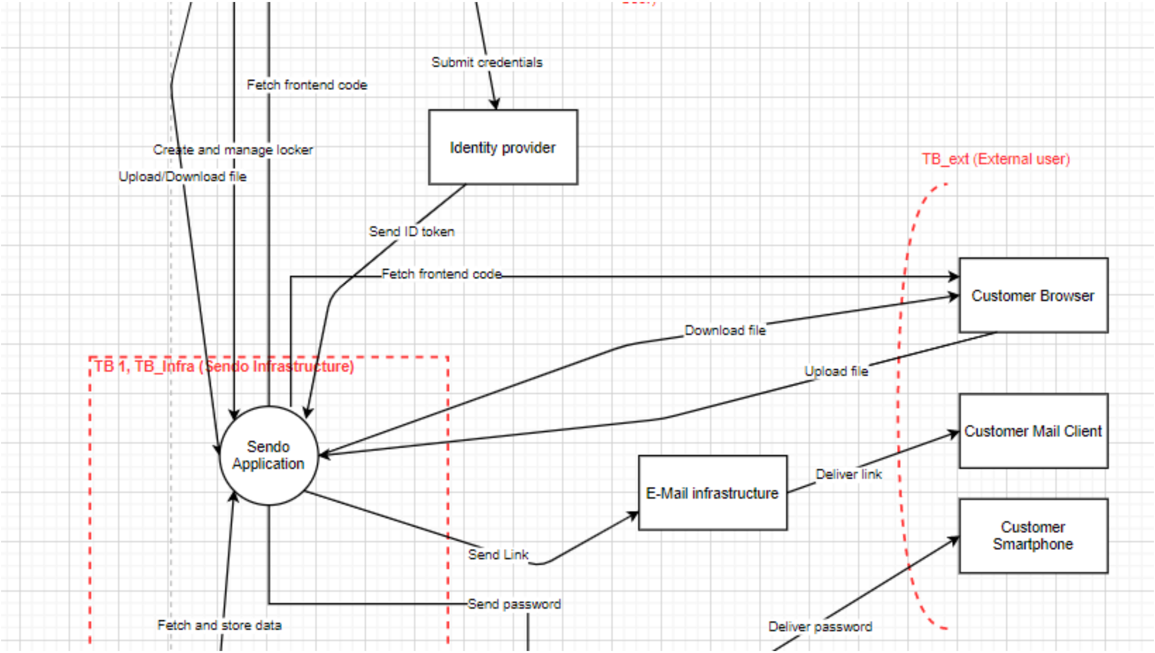
Governance

- Policy & Standards: Internal policy for secure software development
- Compliance Management: ISMS task board with requirements
- Training & Awareness: Our devs regularly visit security conferences and give trainings themselves

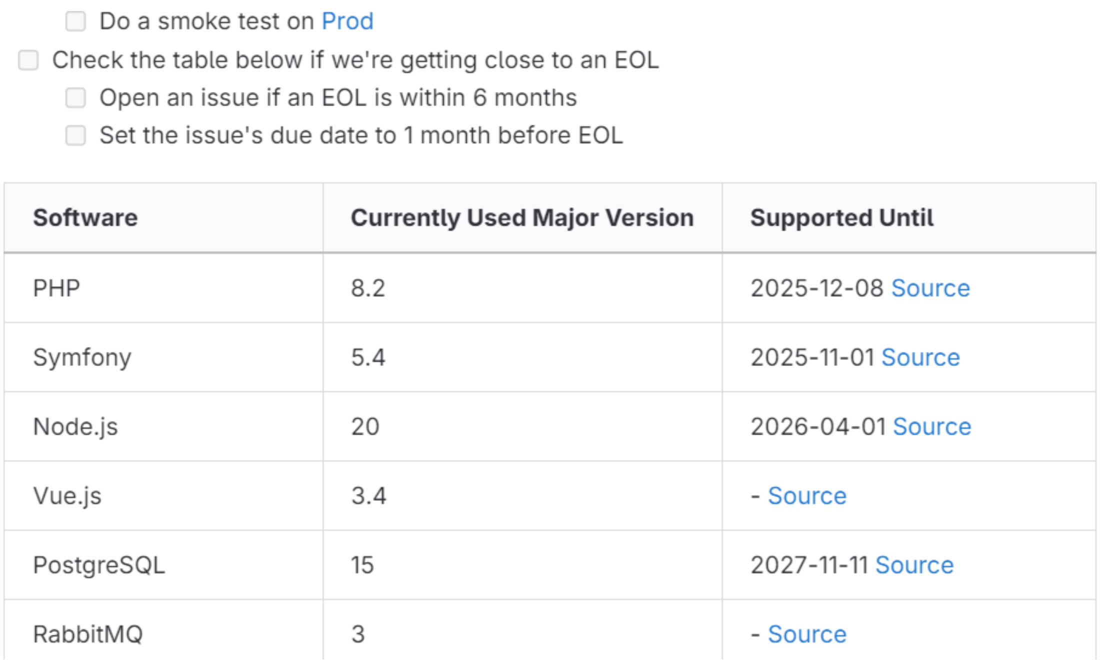
OWASP SAMM At SBA

Design

- Threat Model: Regular assessments conducted
- Architecture Design: We incorporate “Security by default” practices into our design
- Technology Management: We use SBOMs and track our third-party dependencies including the end-of-life dates of large components



Threat Model



  - □ Do a smoke test on Prod
- □ Check the table below if we're getting close to an EOL
  - □ Open an issue if an EOL is within 6 months
  - □ Set the issue's due date to 1 month before EOL

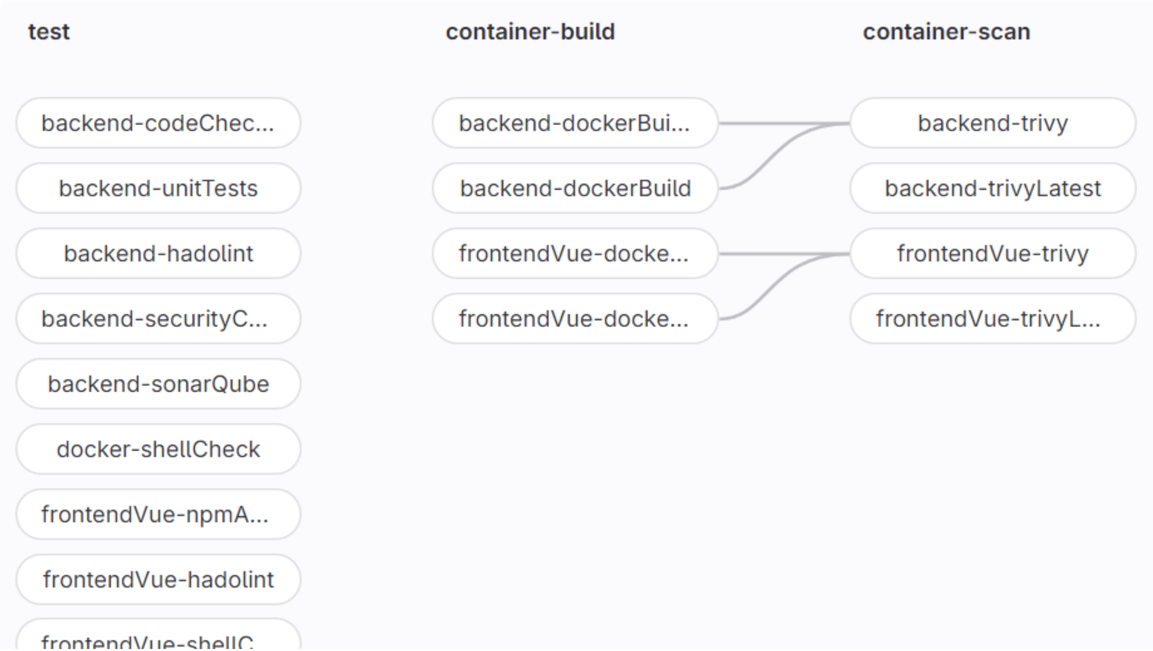
Software	Currently Used Major Version	Supported Until
PHP	8.2	2025-12-08 Source
Symfony	5.4	2025-11-01 Source
Node.js	20	2026-04-01 Source
Vue.js	3.4	- Source
PostgreSQL	15	2027-11-11 Source
RabbitMQ	3	- Source

Tracking of Major Dependency Versions

OWASP SAMM At SBA

Implementation

- Build Process: Completely automated, including security scanners
- Deployment Process: Also completely automated
- Secret Management: We adhere to the principle of least authority



test

- backend-codeChec...
- backend-unitTests
- backend-hadolint
- backend-securityC...
- backend-sonarQube
- docker-shellCheck
- frontendVue-npmA...
- frontendVue-hadolint
- frontendVue-shellC

container-build

- backend-dockerBui...
- backend-dockerBuild
- frontendVue-docke...
- frontendVue-docke...

container-scan

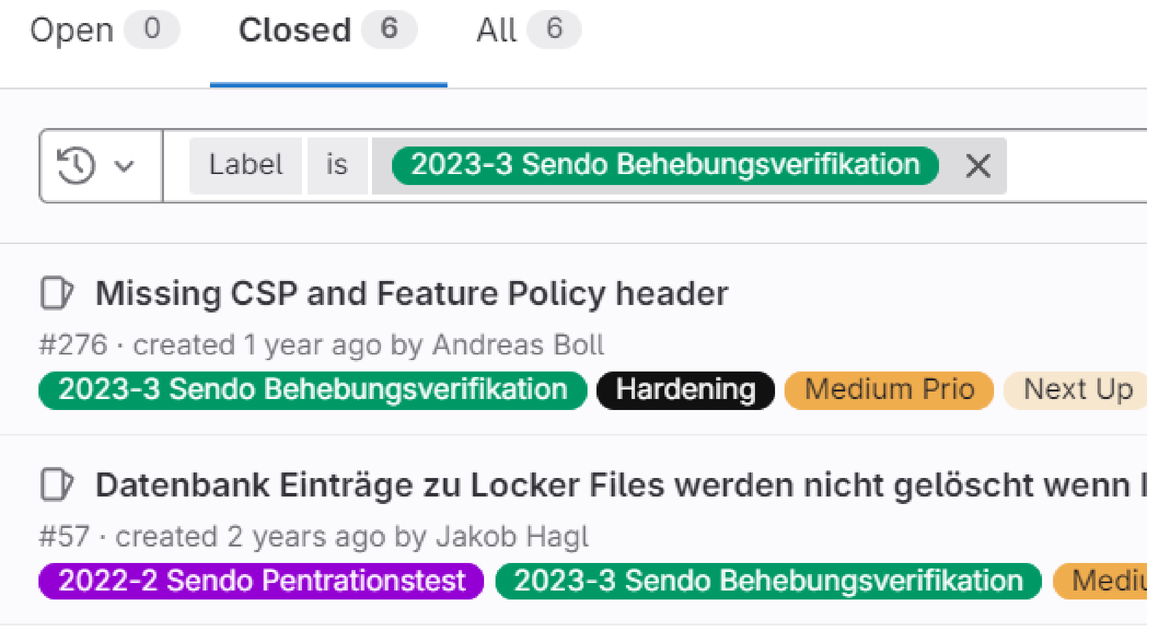
- backend-trivy
- backend-trivyLatest
- frontendVue-trivy
- frontendVue-trivyL...

Automated Build and Deploy Pipelines

OWASP SAMM At SBA

Verification

- Control Verification: We test for security controls and include regression testing
- Scalable Baseline: We have security scanners that test our deployed application daily
- Deep Understanding: We regularly conduct a penetration test from employees outside of the dev team



Open 0 Closed 6 All 6

Label is 2023-3 Sendo Behebungsverifikation

Missing CSP and Feature Policy header

#276 · created 1 year ago by Andreas Boll

2023-3 Sendo Behebungsverifikation Hardening Medium Prio Next Up

Datenbank Einträge zu Locker Files werden nicht gelöscht wenn I

#57 · created 2 years ago by Jakob Hagl

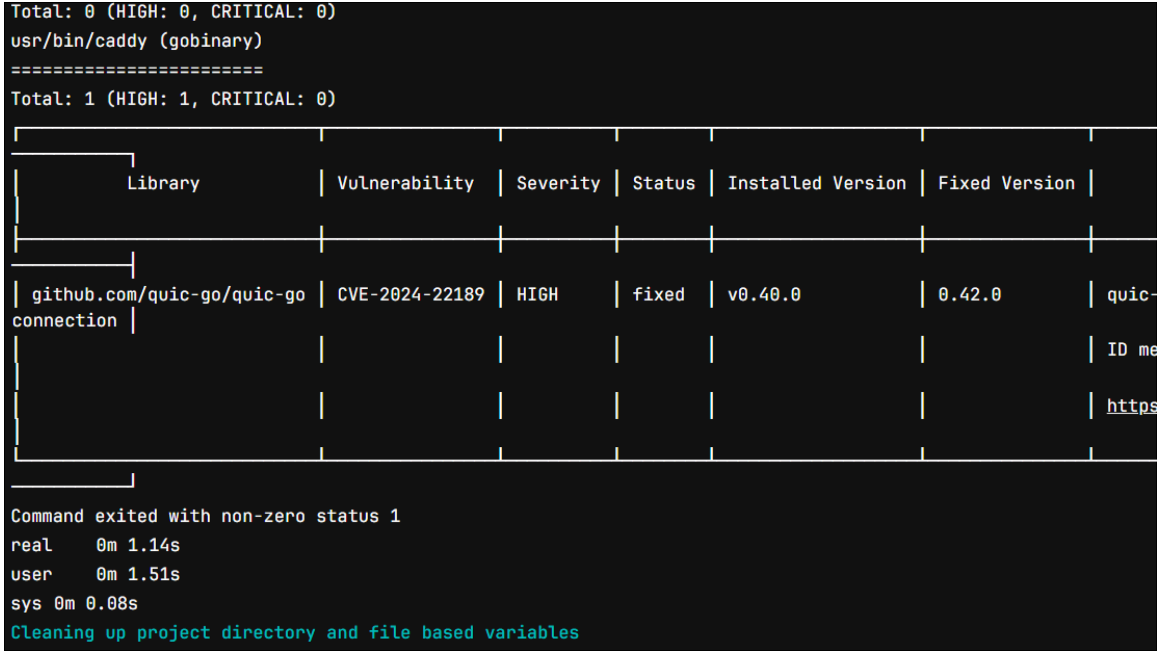
2022-2 Sendo Pentrationstest 2023-3 Sendo Behebungsverifikation Mediu

Penetration Test Findings and Issue Tracking

OWASP SAMM At SBA

Operations

- Incident Detection: Our application is monitored for security events
- Configuration Hardening: We perform best-effort hardenings of the configuration of all components
- Patching and Updating: We monitor the status of our dependencies and alert when vulnerable versions are detected



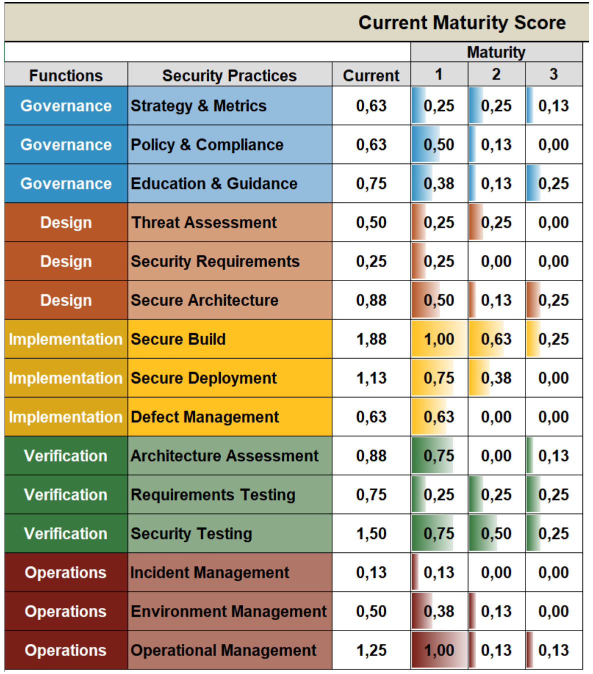
```
Total: 0 (HIGH: 0, CRITICAL: 0)
usr/bin/caddy (gobinary)
========================
Total: 1 (HIGH: 1, CRITICAL: 0)
┌─────────────────────────────┬────────────────┬──────────┬────────┬───────────────────┬───────────────┬────
────────────┐
│           Library           │ Vulnerability  │ Severity │ Status │ Installed Version │ Fixed Version │
│
├─────────────────────────────┼────────────────┼──────────┼────────┼───────────────────┼───────────────┼────
────────────┤
│ github.com/quic-go/quic-go  │ CVE-2024-22189 │ HIGH     │ fixed  │ v0.40.0           │ 0.42.0        │ quic-
connection │
│                             │                │          │        │                   │               │ ID me
│
│                             │                │          │        │                   │               │ https
│
└─────────────────────────────┴────────────────┴──────────┴────────┴───────────────────┴───────────────┴────
────────────┘
Command exited with non-zero status 1
real    0m 1.14s
user    0m 1.51s
sys 0m 0.08s
Cleaning up project directory and file based variables
```

Scans for Vulnerable Dependency Versions

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

Assessment Types

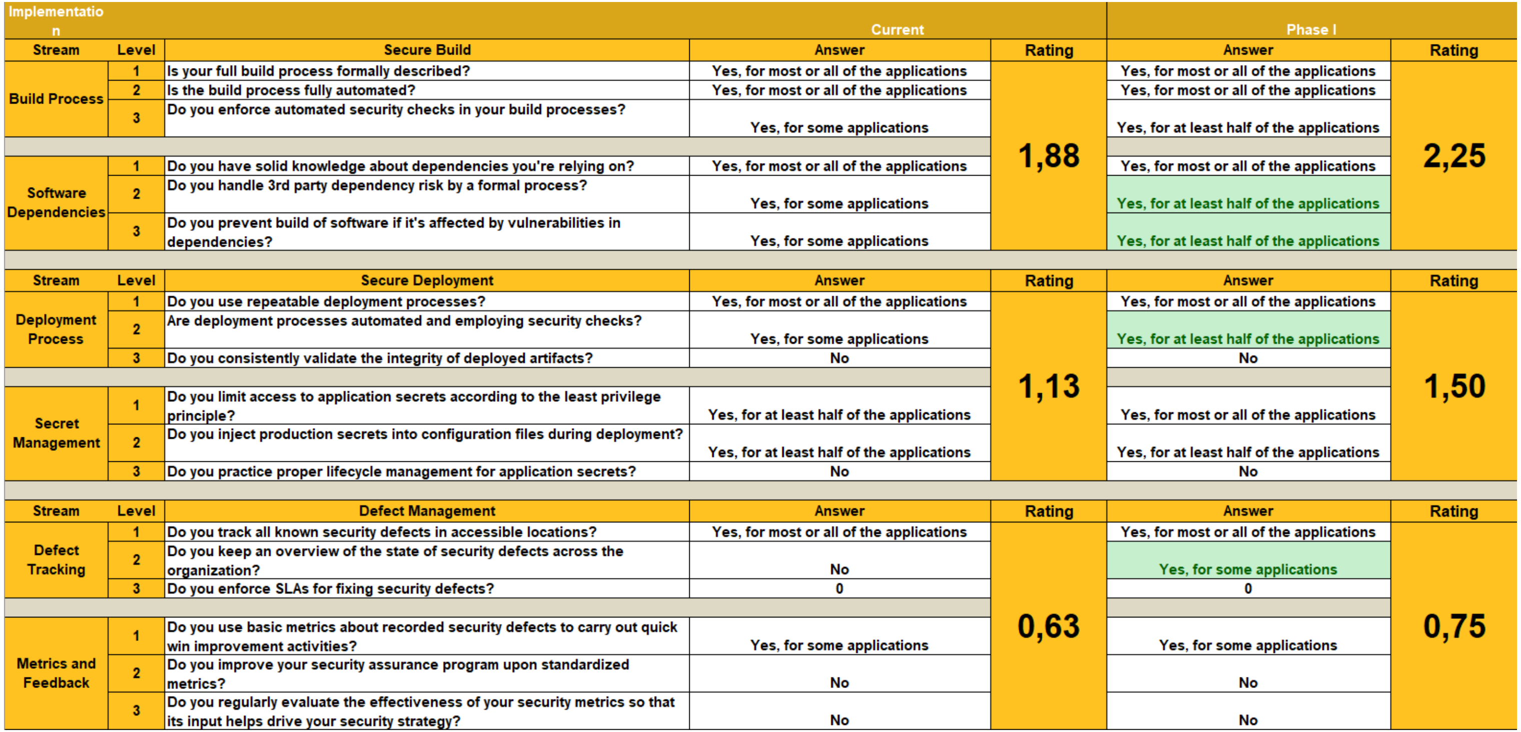
- **External interviewers**
  - Security experts are interviewers
  - Report with suggestions for moving forward
- **Self assessment**
  - Interview done by the team itself
  - Much faster since no evidence is collected
  - Can be done more often

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

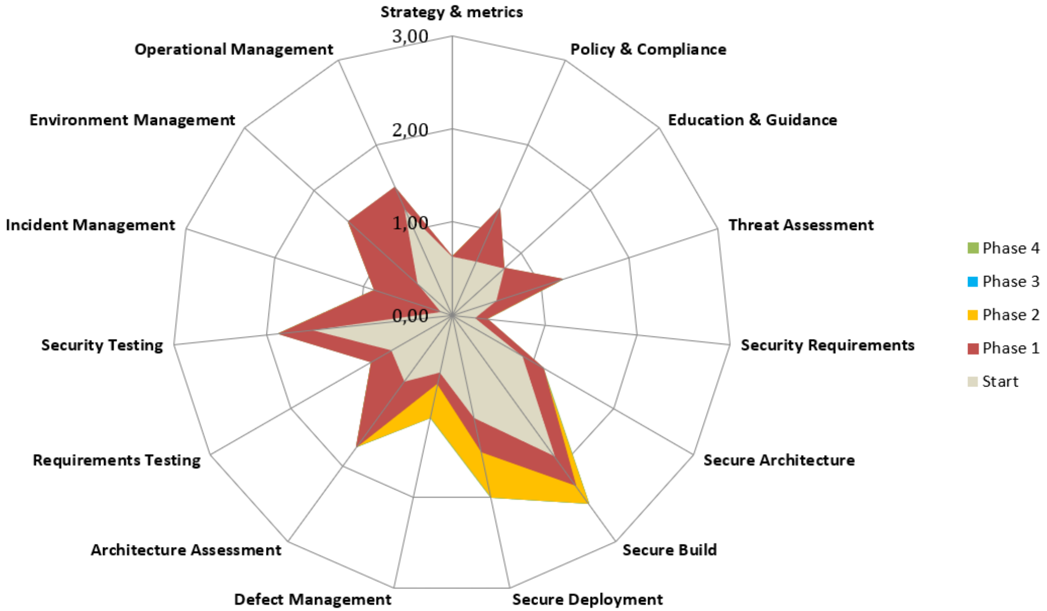
Roadmap



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



Stefan Jakoubi and Michael Koppmann

SBA Research

Floragasse 7, 1040 Vienna

sjakoubi@sba-research, mkoppmann@sba-research.org

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