Maxim Baele

Volunteer

OWASP Belgium chapter leader

OWASP SAMM core team member

OWASP Regulations & Standards Liaison

→ Bridge-builder

ORC-WG (Resources)

Maxim Baele

Principal Consultant Product Security @TOREON

Tinkering with Linux

Linux system engineering

Automation

Build systems (CI/CD)

… and product security

Can you help us build secure products?

… and product security

How to draw an owl

1. Draw some circles

2. Draw the rest of the fucking owl

How to build secure products

1. Draft some policies

2. Build secure products

OWASP SAMM

Open Worldwide Application Security Project
 °2001

Tools, guidance, standards, community

Project-based

OWASP SAMM

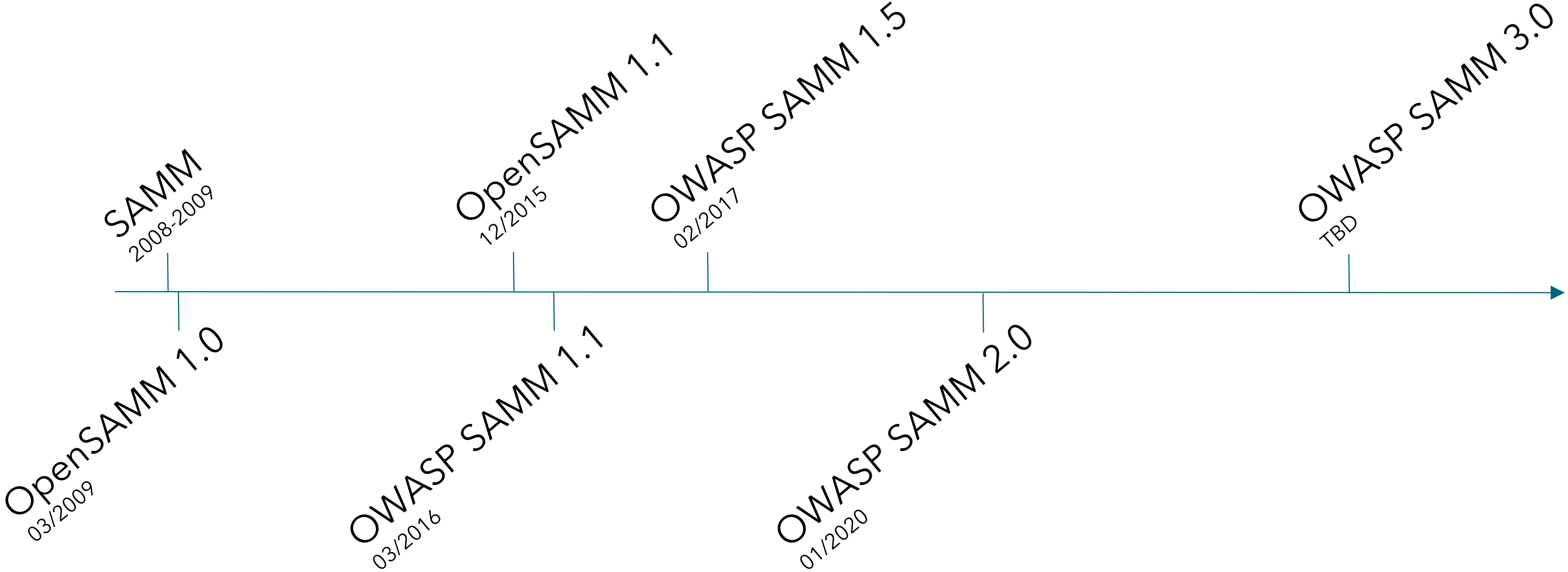
Software Assurance Maturity Model

V1 in 2009, now at version 2.1.0

Prescriptive standard (Opinionated!)

Implementation tool to help you prepare for product security certifications and legislative compliance

https://owaspsamm.org



SAMM
2008-2009

OpenSAMM 1.0
03/2009

OpenSAMM 1.1
12/2015

OWASP SAMM 1.1
03/2016

OWASP SAMM 1.5
02/2017

OWASP SAMM 2.0
01/2020

OWASP SAMM 3.0
TBD

Microsoft SDL

† Cigital Security Touchpoints

† OWASP CLASP

BSIMM

NIST SP800-218 SSDF

(ISO 27034)

75

All core team members are practitioners themselves

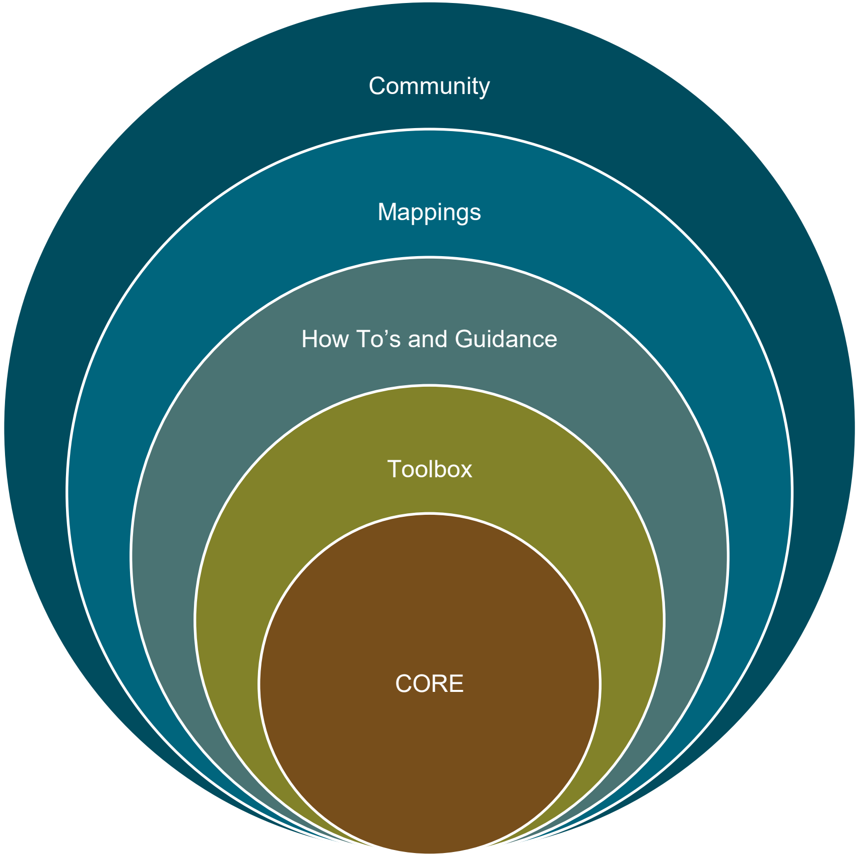
Experts contribute to core team guidance (e.g. agile guidance)

Practitioners contribute to community guidance

Work happens in public

https://github.com/owaspsamm/
https://www.meetup.com/owasp-samm/
https://owasp.slack.com/messages/C0VF1EJGH

→ Community-driven improvements

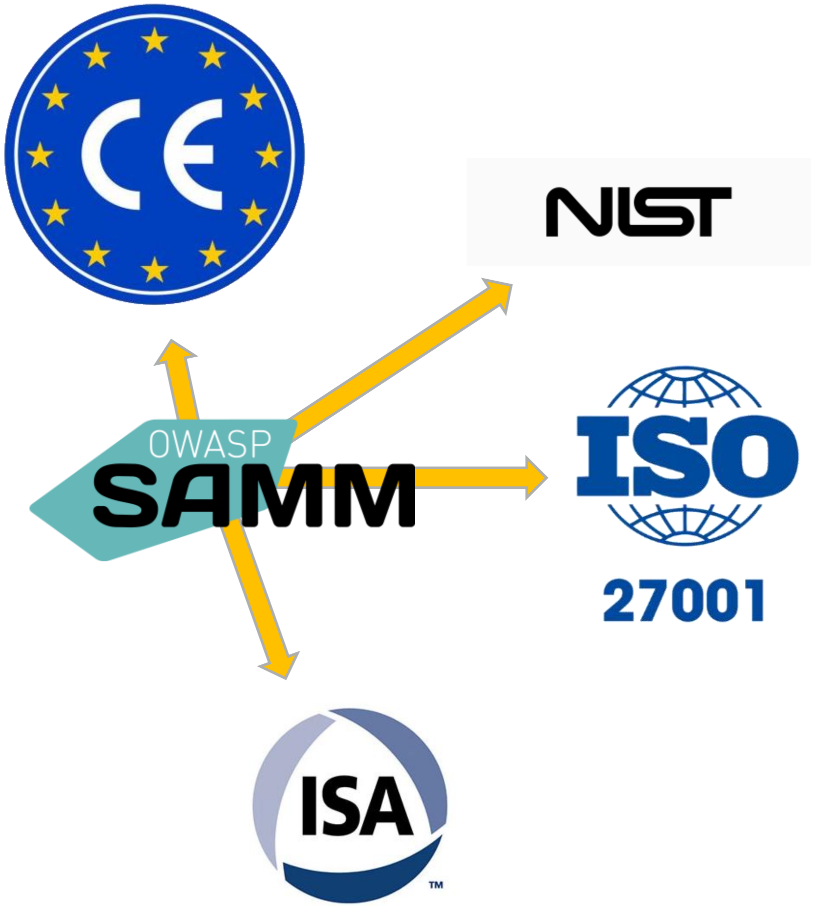


Stable Core & Toolbox
→ automation-friendly

Continuously expanding guidance

Growing set of mappings

Helpful community
& growing set of experts



- NIST SSDF (Co-op with NIST)
- OpenCRE → opencre.org
- ISO 27002:2022
- BSIMM13 & 14
- IEC62443-4-1
- EU Cyber Resilience Act
- Microsoft SDL
- NIST CSF
- NIST SP800-53 rev 5
- ?

Declaration of Conformity

Technical Documentation

Declaration of Conformity

Technical Documentation

Vulnerability Management

Declaration of Conformity

Technical Documentation

Vulnerability Management

Secure by design, based on risk analysis

Released without known, exploitable vulnerabilities
Adhering to high-level Technical Requirements
Patchable

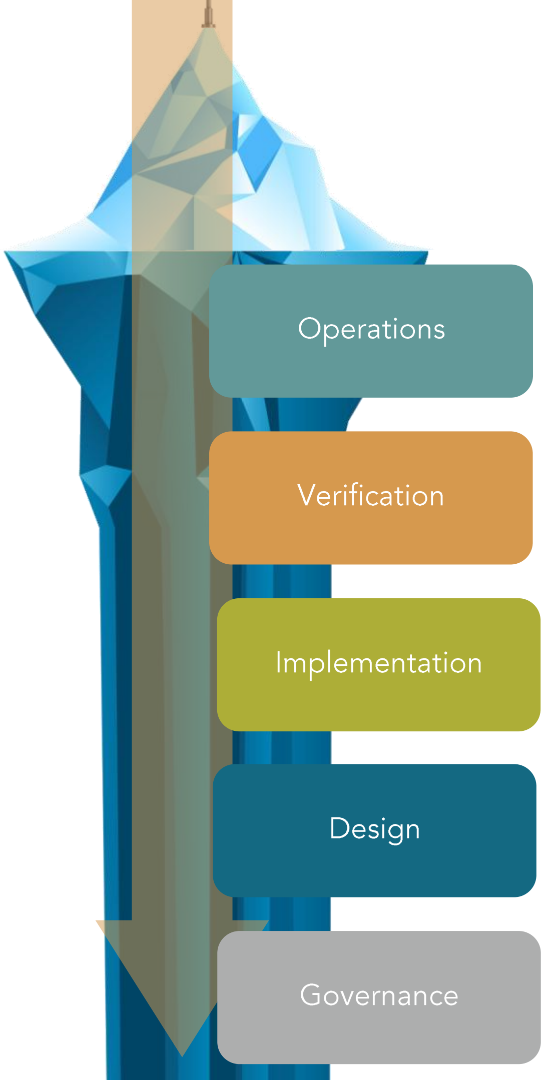
Declaration of Conformity

Technical Documentation

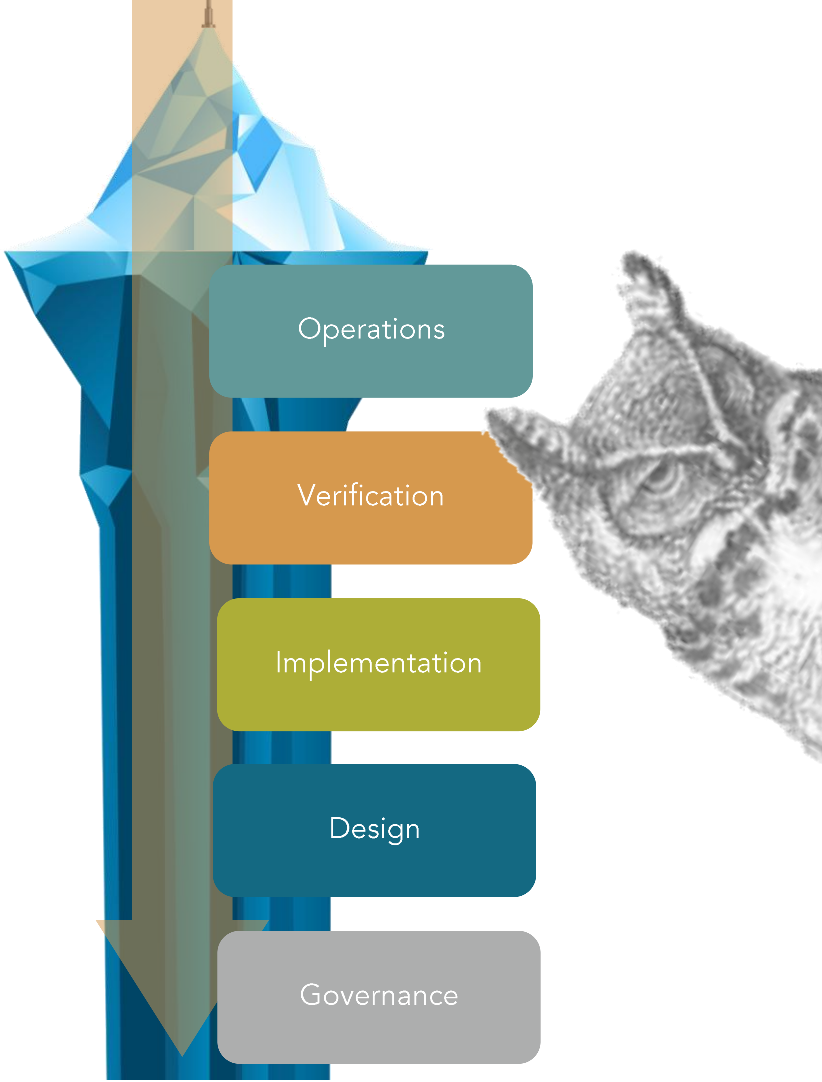
Vulnerability Management

Secure by design, based on risk analysis

Released without known, exploitable vulnerabilities
Adhering to high-level Technical Requirements
Patchable



Secure Development Lifecycle



Operations

Verification

Implementation

Design

Governance

Governance

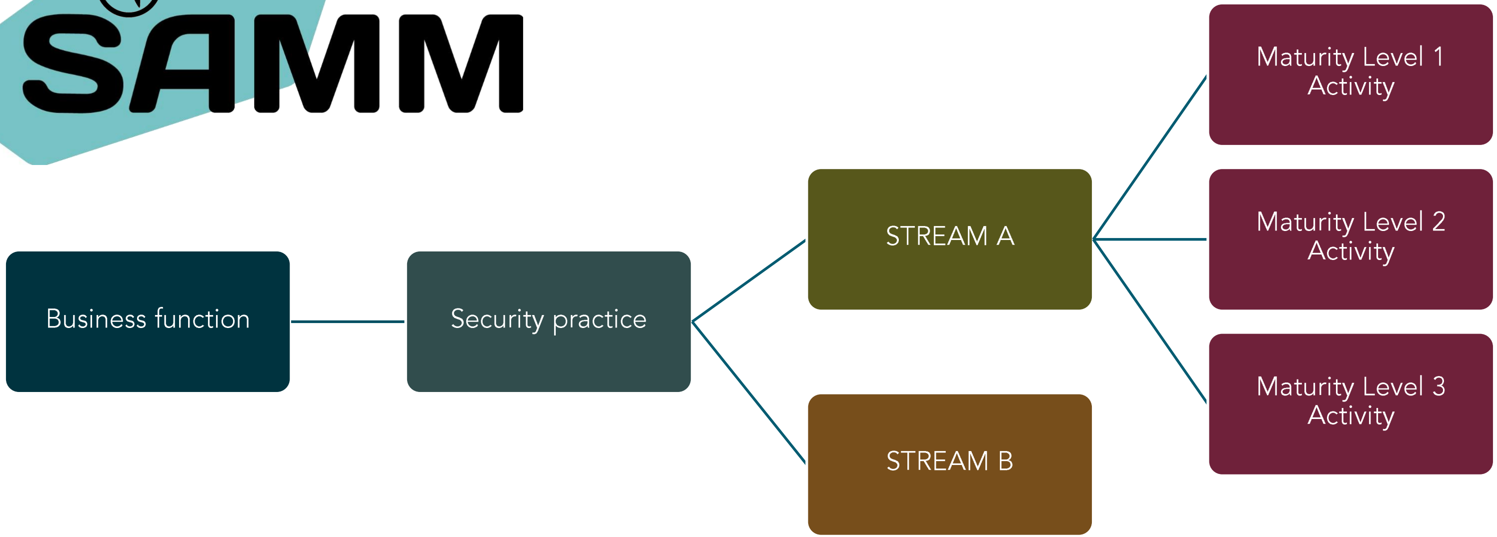
Design

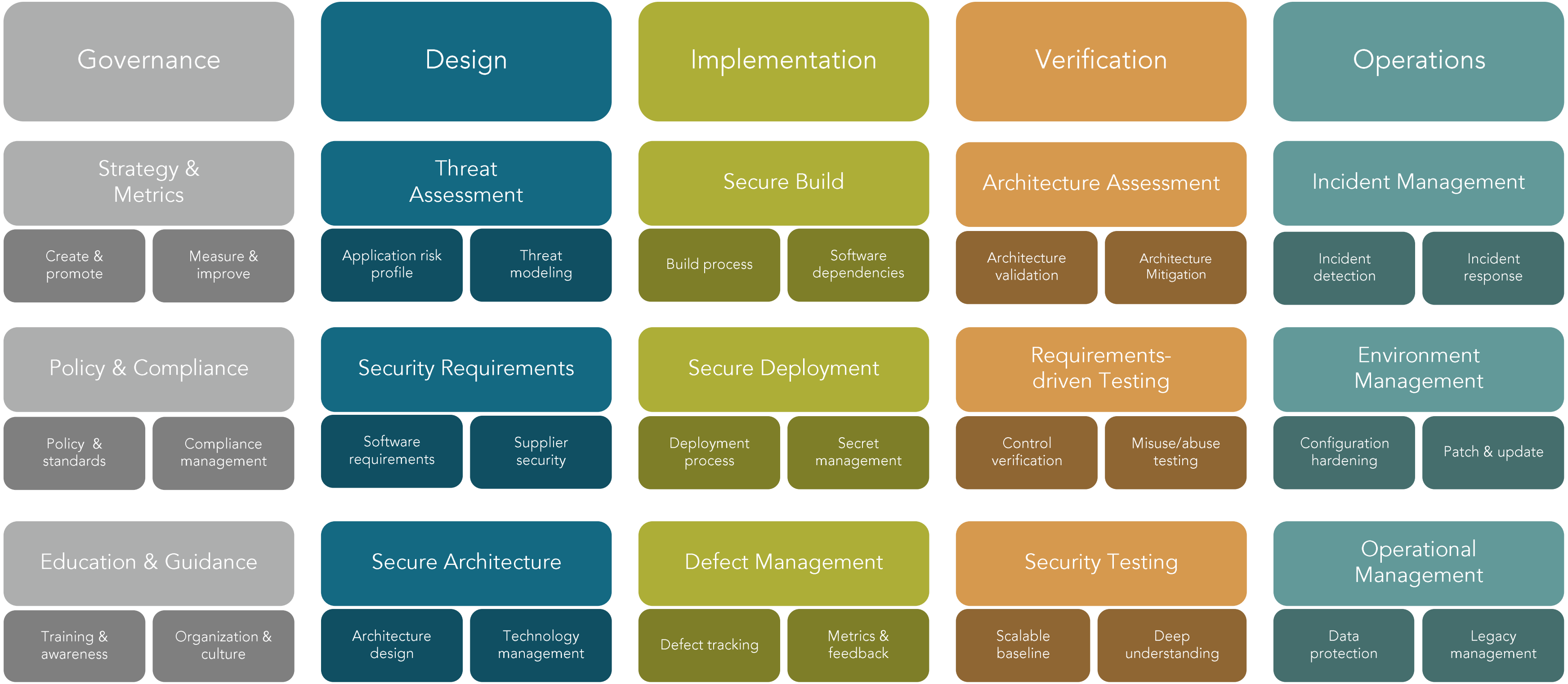
Implementation

Verification

Operations

OWASP SAMM


Business function
Security practice
STREAM A
STREAM B
Maturity Level 1 Activity
Maturity Level 2 Activity
Maturity Level 3 Activity



Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Create & promote Measure & improve	Application risk profile Threat modeling	Build process Software dependencies	Architecture validation Architecture Mitigation	Incident detection Incident response
Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Policy & standards Compliance management	Software requirements Supplier security	Deployment process Secret management	Control verification Misuse/abuse testing	Configuration hardening Patch & update
Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management
Training & awareness Organization & culture	Architecture design Technology management	Defect tracking Metrics & feedback	Scalable baseline Deep understanding	Data protection Legacy management

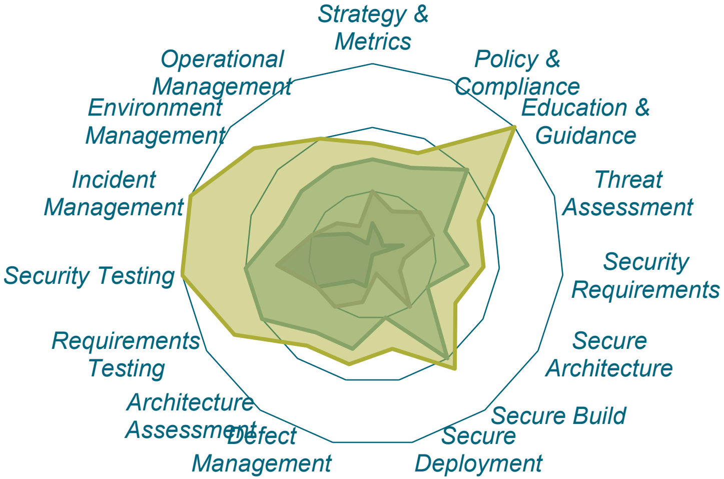
Maturity levels

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

Assessment tooling

https://owaspsamm.org/assessment

→ SAMM Toolbox
→ Sammy (Codific)
→ SAMMwise



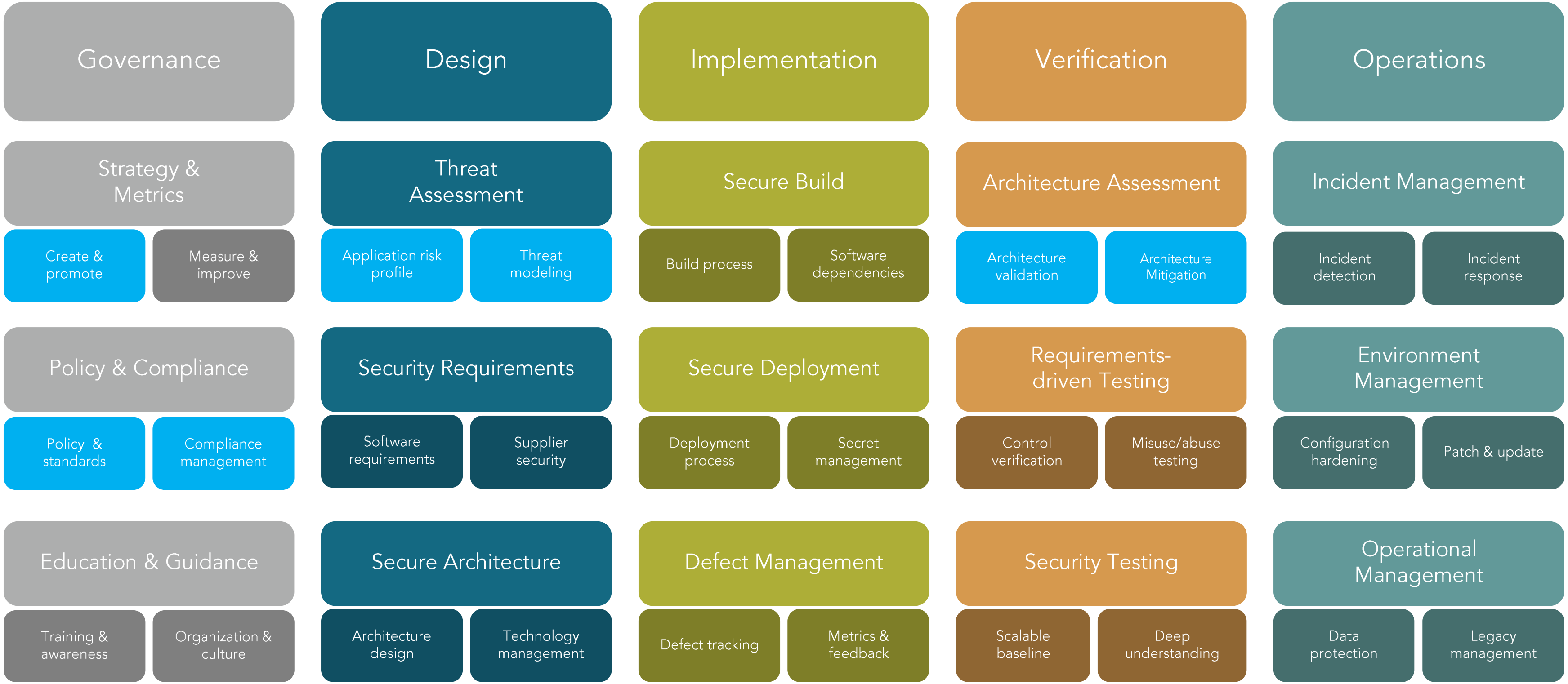
Secure Development Lifecycle

Secure by design, based on risk analysis

Released without known, exploitable vulnerabilities
Adhering to high-level Technical Requirements
Patchable

Vulnerability handling

Secure by design, based on risk analysis

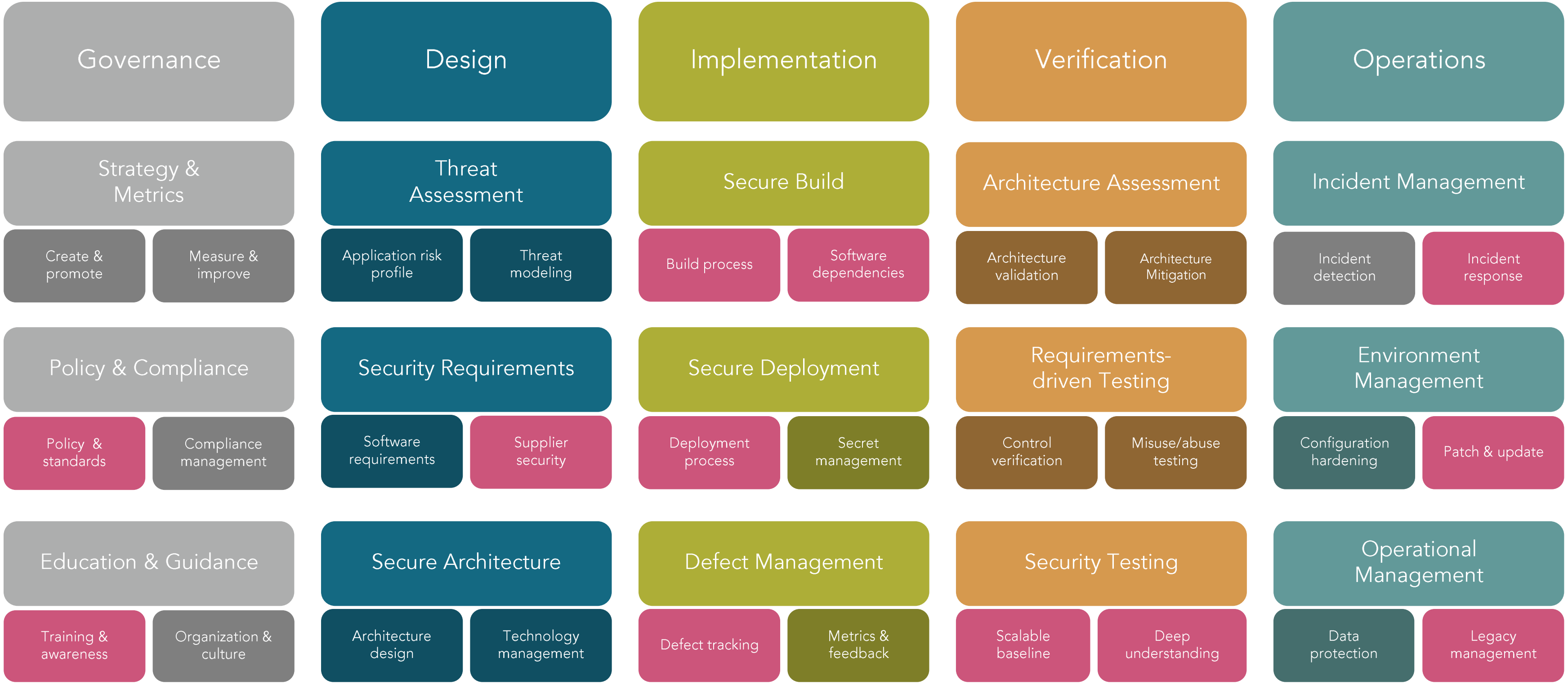


Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Create & promote	Application risk profile	Build process	Architecture validation	Incident detection
Measure & improve	Threat modeling	Software dependencies	Architecture Mitigation	Incident response
Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Policy & standards	Software requirements	Deployment process	Control verification	Configuration hardening
Compliance management	Supplier security	Secret management	Misuse/abuse testing	Patch & update
Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management
Training & awareness	Architecture design	Defect tracking	Scalable baseline	Data protection
Organization & culture	Technology management	Metrics & feedback	Deep understanding	Legacy management

Released without known, exploitable vulnerabilities
Adhering to high-level Technical Requirements
Patchable

Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Create & promote Measure & improve	Application risk profile Threat modeling	Build process Software dependencies	Architecture validation Architecture Mitigation	Incident detection Incident response
Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Policy & standards Compliance management	Software requirements Supplier security	Deployment process Secret management	Control verification Misuse/abuse testing	Configuration hardening Patch & update
Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management
Training & awareness Organization & culture	Architecture design Technology management	Defect tracking Metrics & feedback	Scalable baseline Deep understanding	Data protection Legacy management

Vulnerability handling



Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Create & promote Measure & improve	Application risk profile Threat modeling	Build process Software dependencies	Architecture validation Architecture Mitigation	Incident detection Incident response
Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Policy & standards Compliance management	Software requirements Supplier security	Deployment process Secret management	Control verification Misuse/abuse testing	Configuration hardening Patch & update
Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management
Training & awareness Organization & culture	Architecture design Technology management	Defect tracking Metrics & feedback	Scalable baseline Deep understanding	Data protection Legacy management

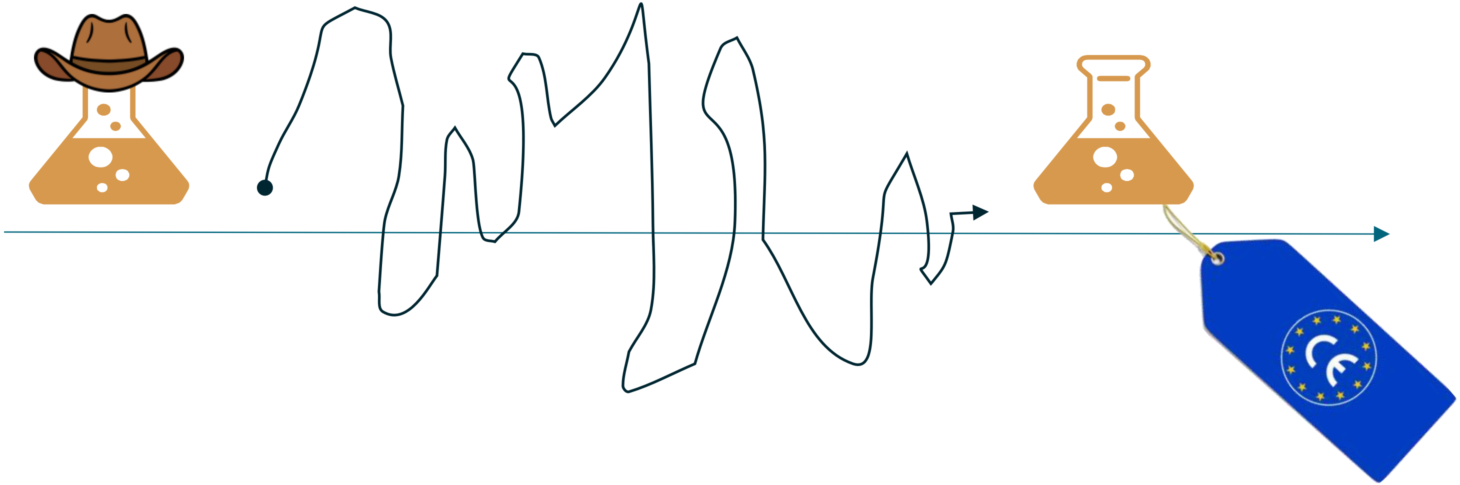
Do you classify applications according to business risk based on a simple and predefined set of questions?		
An agreed-upon risk classification exists	Yes	A clear and simple risk classification system is in place, at minimum aligning with CRA product classification categories. All products are classified, including existing and legacy applications.
The application team understands the risk classification	Yes	Application risk classification is part of security training, explaining both the classification scheme and the implications for products.
The risk classification covers critical aspects of business risks the organization is facing	Yes	Non-compliancies to CRA obligations are classified as business risks.
The organization has an inventory for the applications in scope	Yes	The inventory is centrally documented (see L2 requirements), linked to context defined in G-SM-A and requirements defines in G-PC-B

→ Product Security Strategy

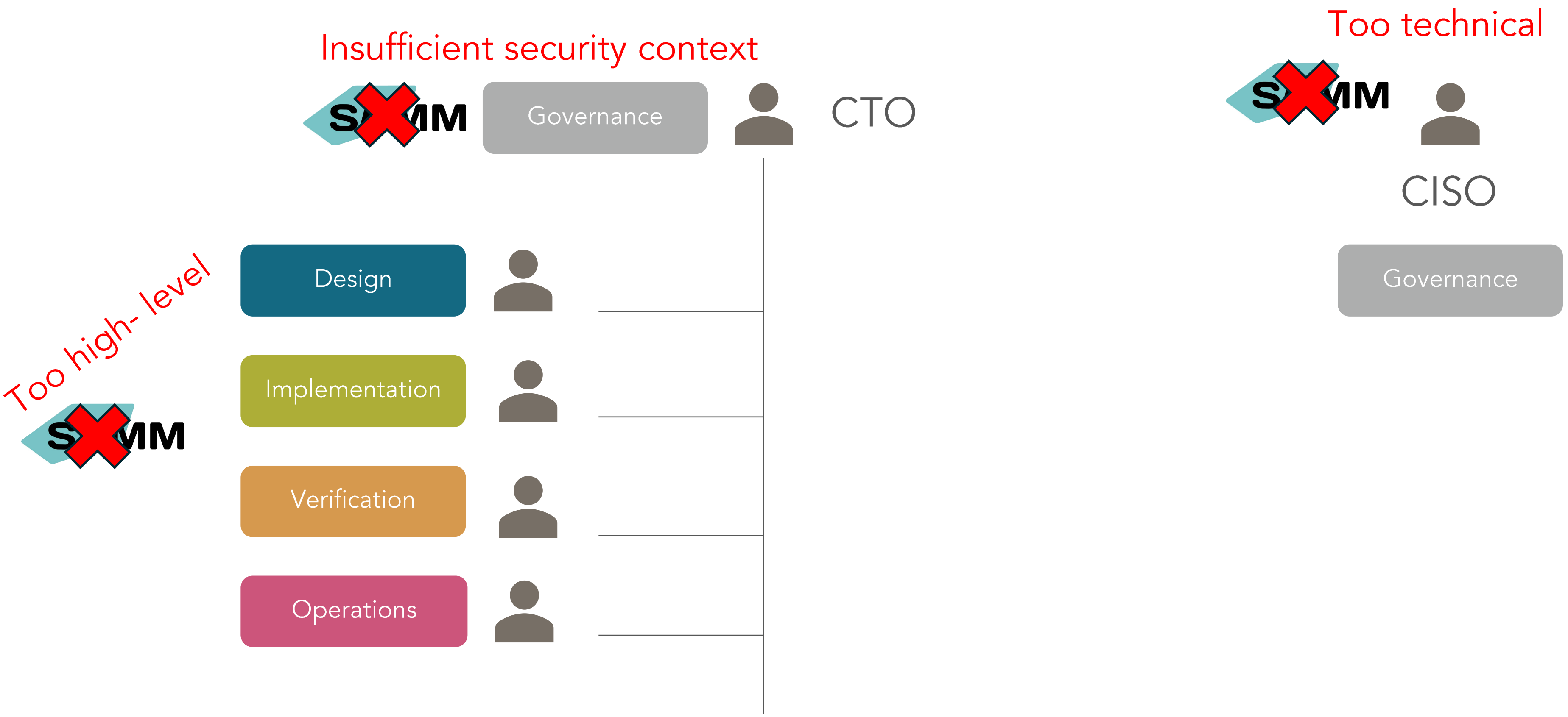
“Supporting Activities”

Governance	Design	Implementation	Verification	Operations
Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Create & promote Measure & improve	Application risk profile Threat modeling	Build process Software dependencies	Architecture validation Architecture Mitigation	Incident detection Incident response
Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Policy & standards Compliance management	Software requirements Supplier security	Deployment process Secret management	Control verification Misuse/abuse testing	Configuration hardening Patch & update
Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management
Training & awareness Organization & culture	Architecture design Technology management	Defect tracking Metrics & feedback	Scalable baseline Deep understanding	Data protection Legacy management

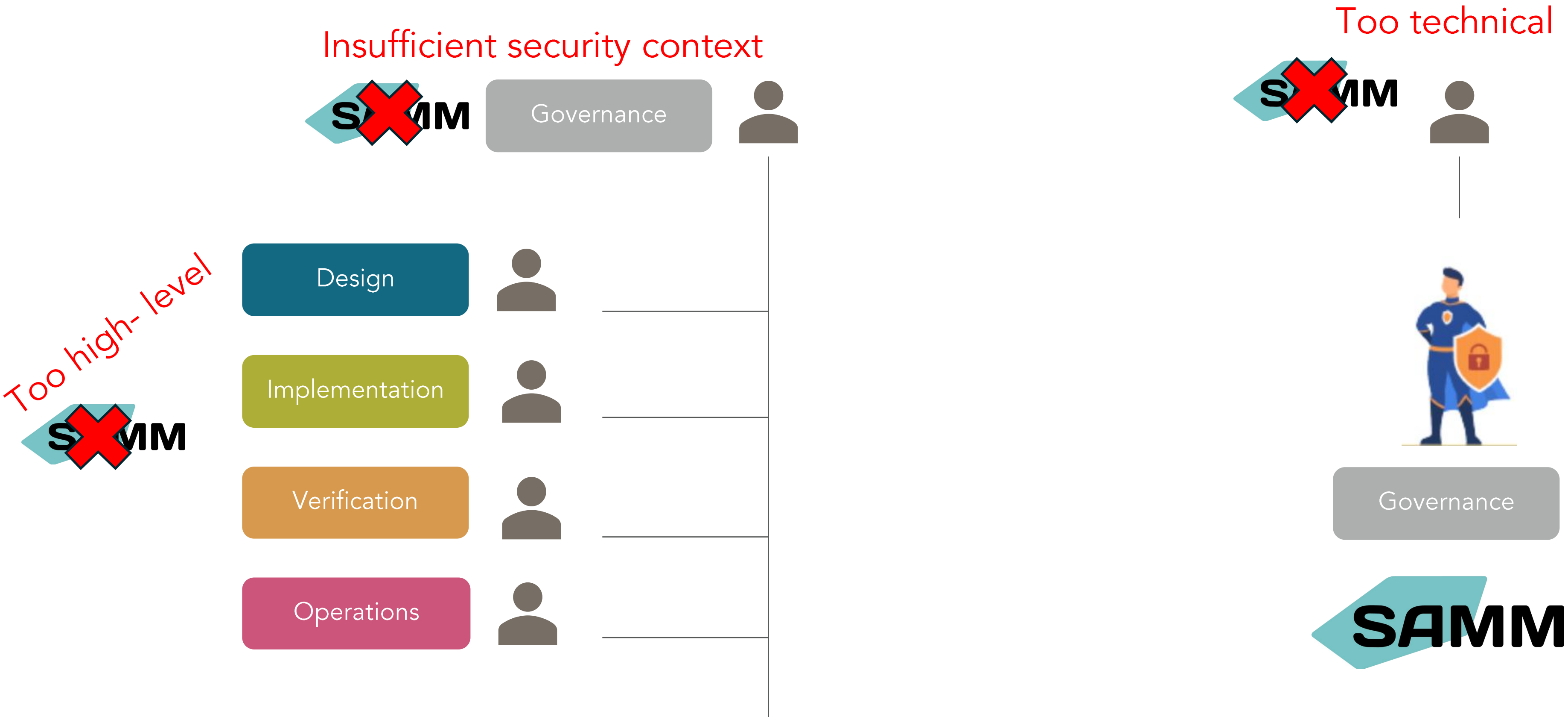
→ Product Security Strategy



Who Owns Product Security Strategy?



Who Owns Product Security Strategy?



Insufficient security context

Too technical

Too high- level

Governance

Design

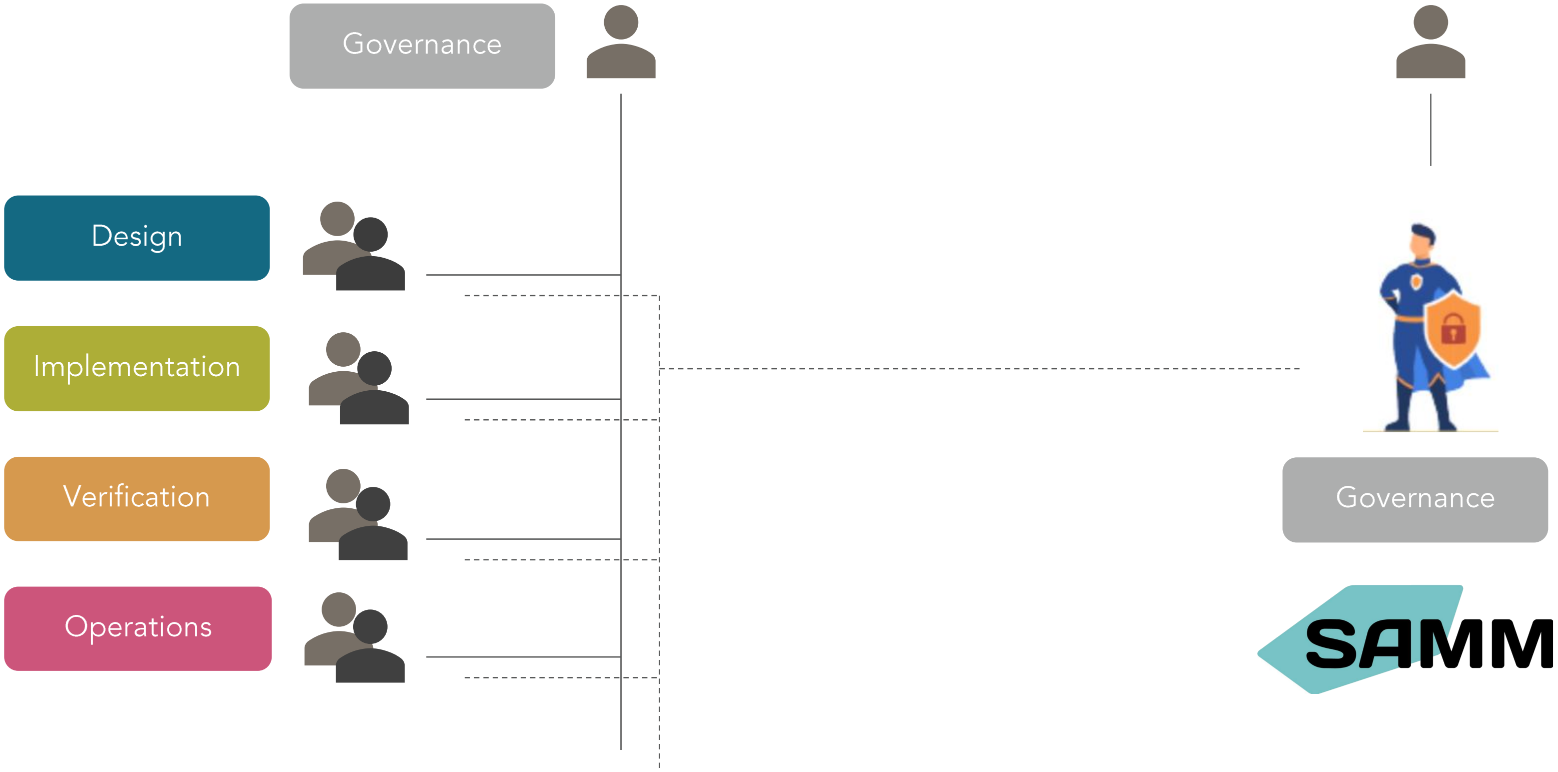
Implementation

Verification

Operations

Governance

Who Owns Product Security Strategy?



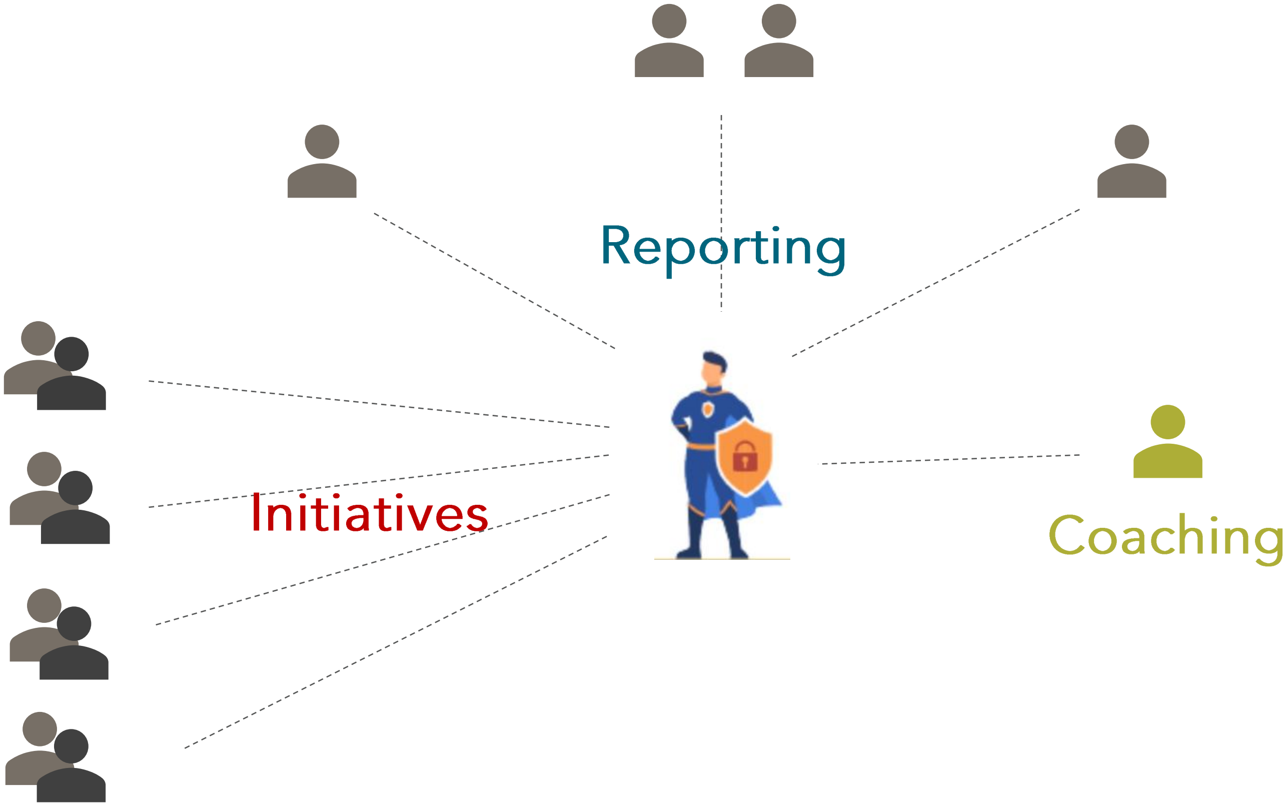
Who Owns Product Security Strategy?

Technical background

- CTO, Architect, Lead Developer
- Product Security [Architect|Officer|Manager|…]

Security Champion

- Advisory role!
- Assistance from legal
- Supported by the full organization



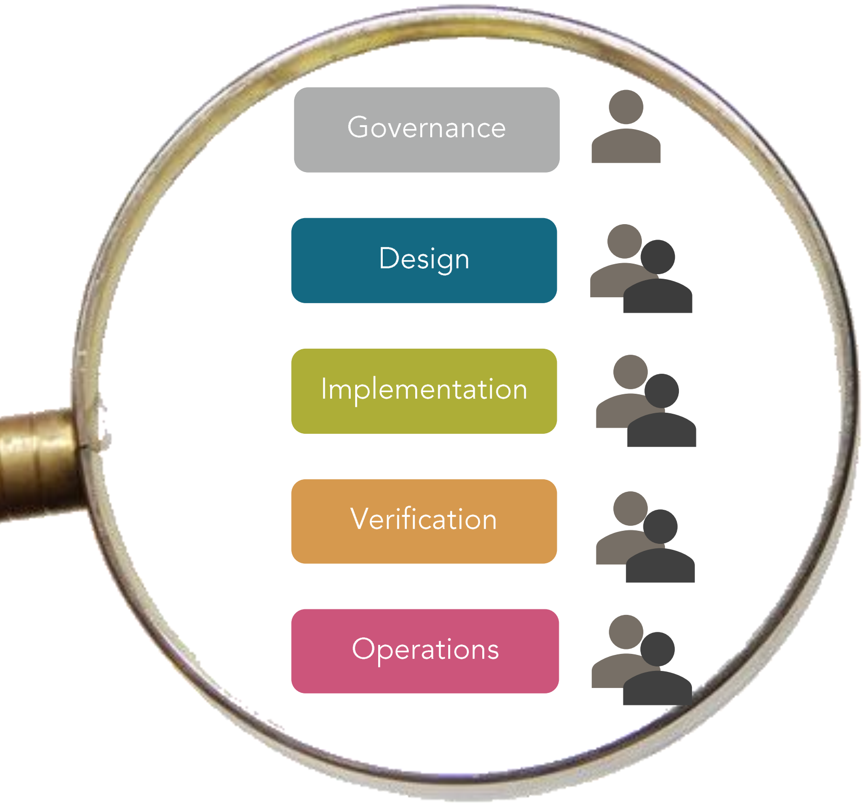
Reporting

Initiatives

Coaching

Scope

SAMM



Focused on a single product

…or similar set of products

Taking part in the same SDLC

SAMM

Governance

Design

Implementation

Verification

Operations

Company History

Active markets and industries

Organizational Structure

Internal & External Drivers for security

Efforts and initiatives thus far

Historic Incidents

Context

SAMM

Governance

Design

Implementation

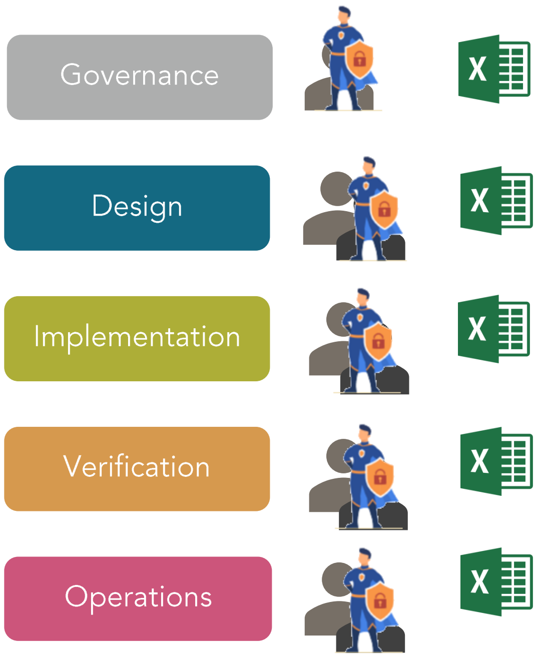
Verification

Operations

Getting Data

Getting Data

SAMM



Governance

Design

Implementation

Verification

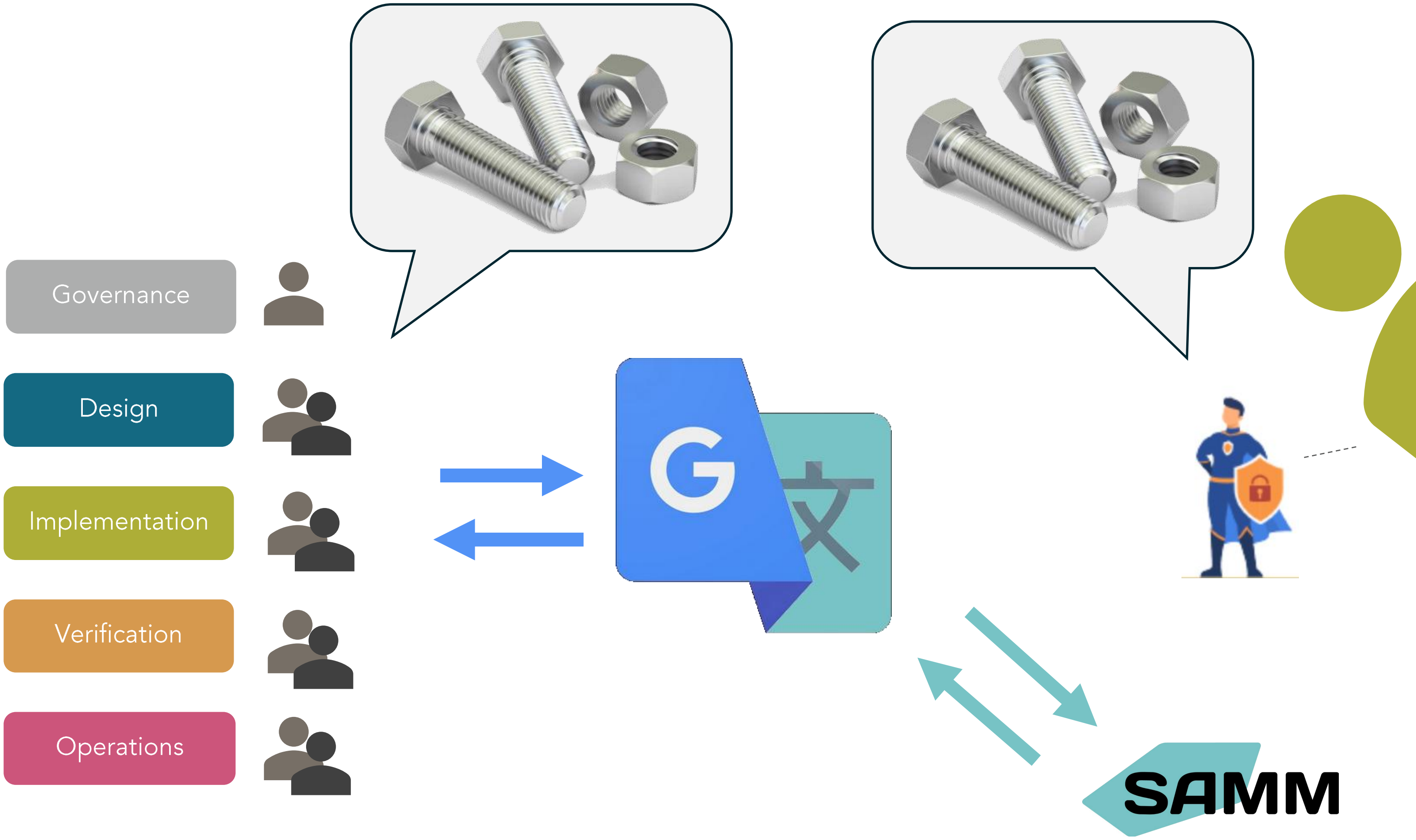
Operations

In-depth knowledge of SAMM required

Inconsistencies!

→(Very) mature organizations

→*Still not recommended*



Governance

Design

Implementation

Verification

Operations

SAMM

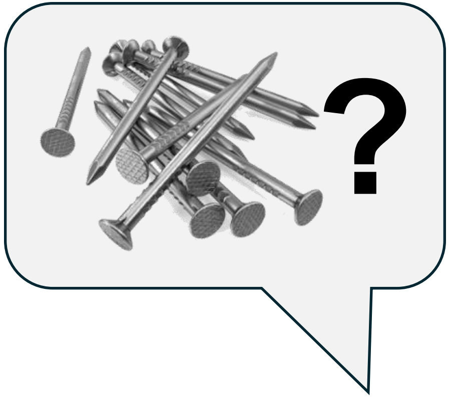
Governance

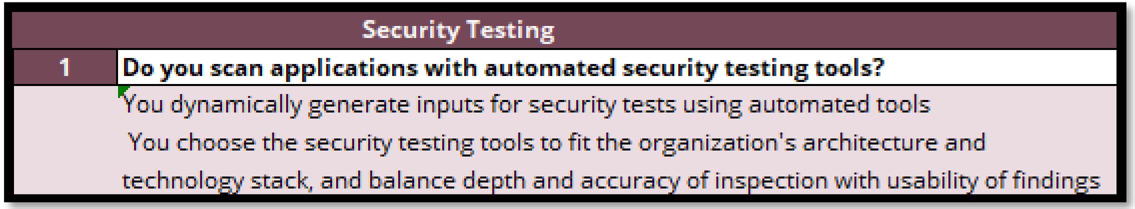
Design

Implementation

Verification

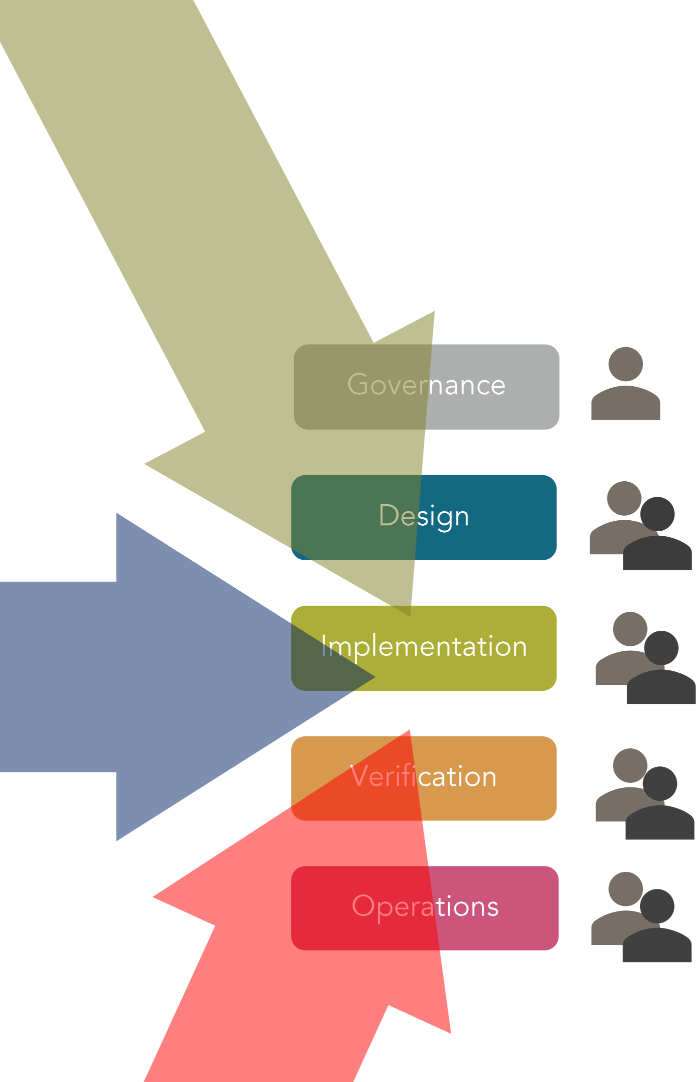
Operations

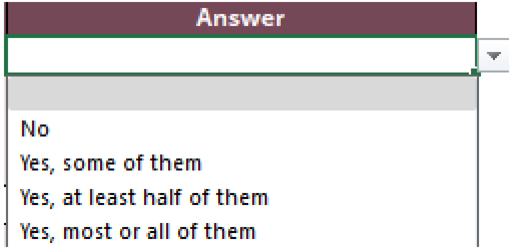




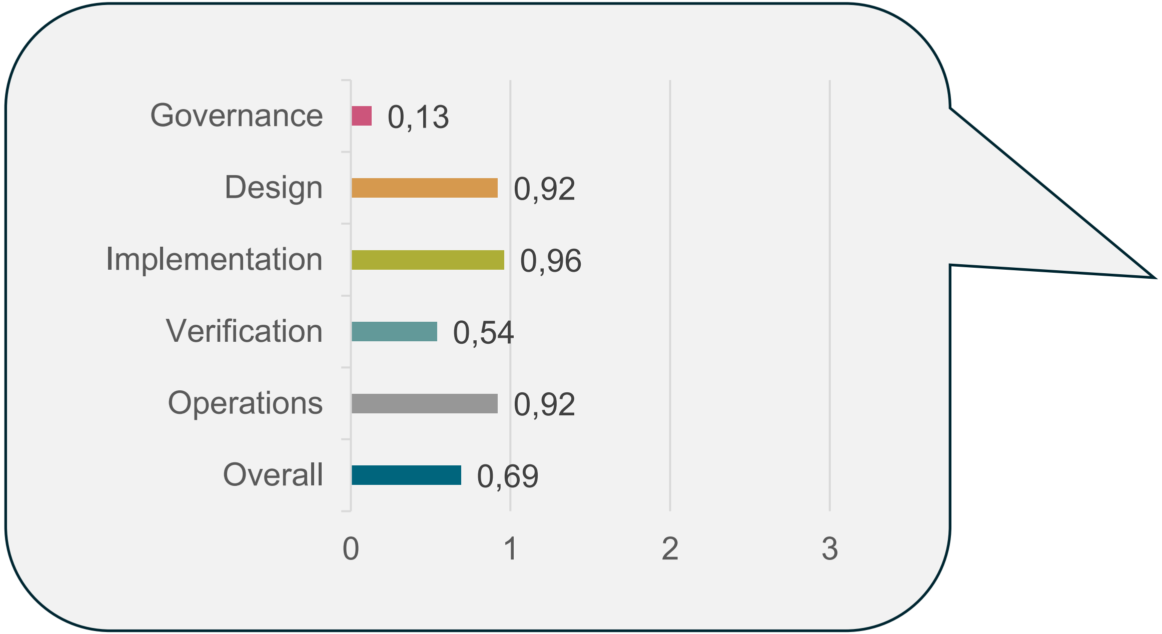
Security Testing	
1	**Do you scan applications with automated security testing tools?**
	You dynamically generate inputs for security tests using automated tools You choose the security testing tools to fit the organization's architecture and technology stack, and balance depth and accuracy of inspection with usability of findings

ESTWING
DEWALT




Answer

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



SCORES ARE RELATIVE

SCORES ARE RELATIVE

…to the organization’s risk appetite

…to the team’s maturity

…to a point in time

…to the assessor (in some cases)

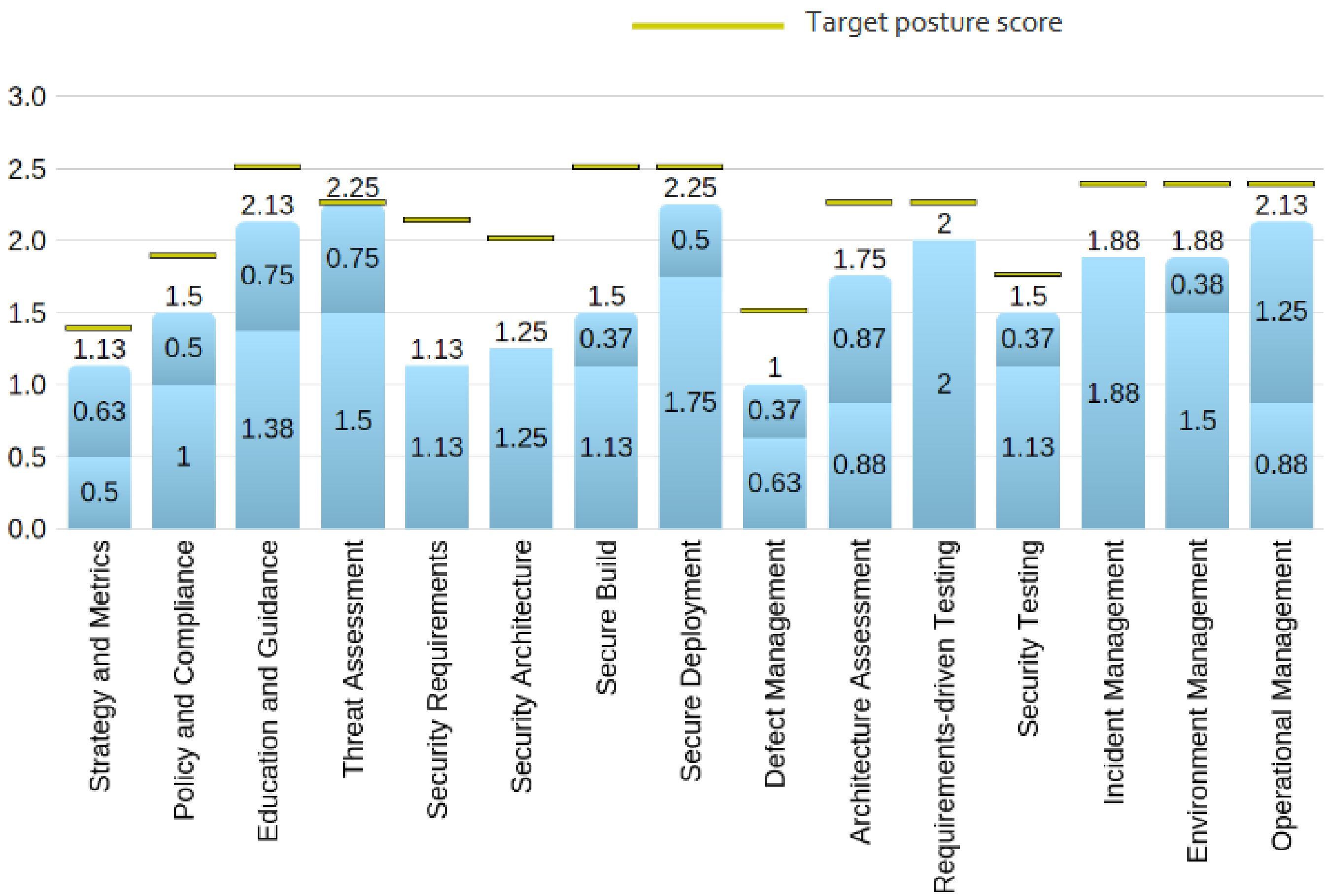
TARGETS ARE RELATIVE

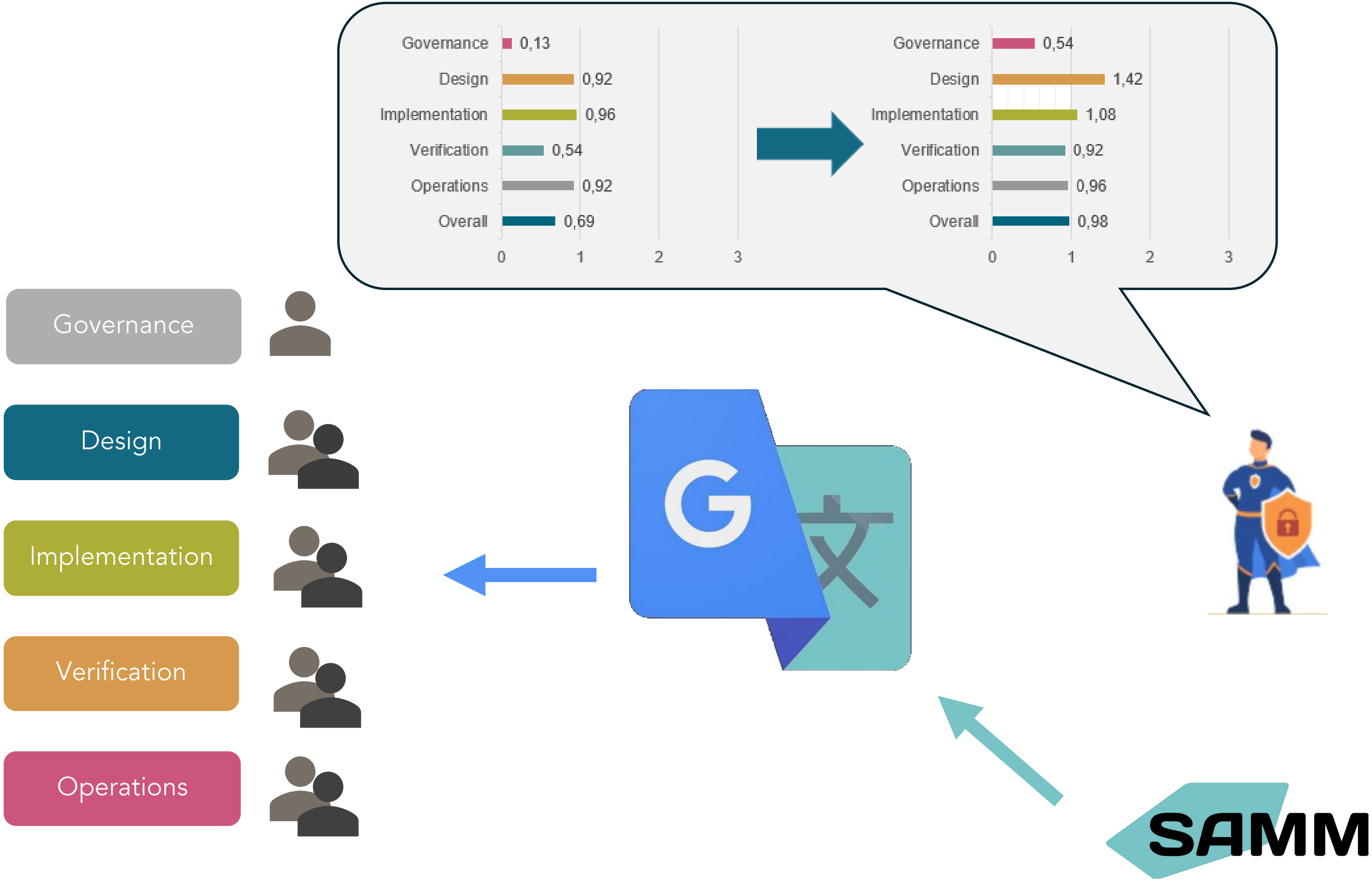
…to the capacity for change

…to market and legislatory demands

…to the lifecycle of the product(s) in scope

Per practice





Governance

Design

Implementation

Verification

Operations

THE TEAM OWNS THE ROADMAP

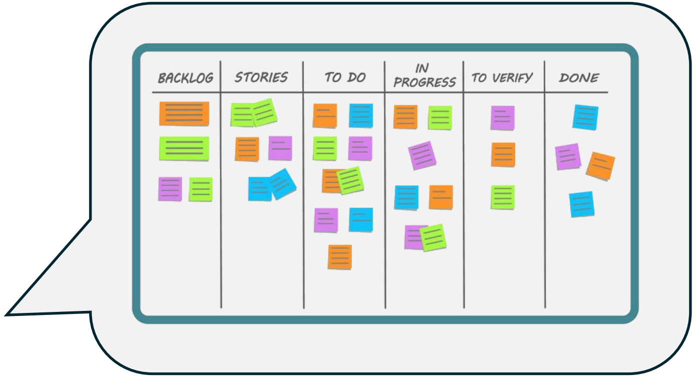
Governance

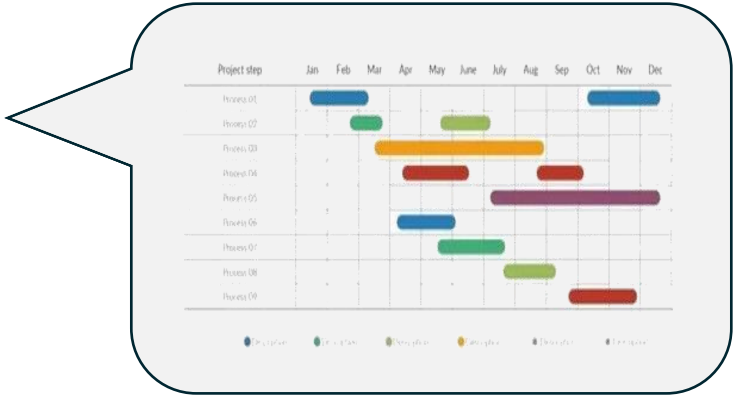
Design

Implementation

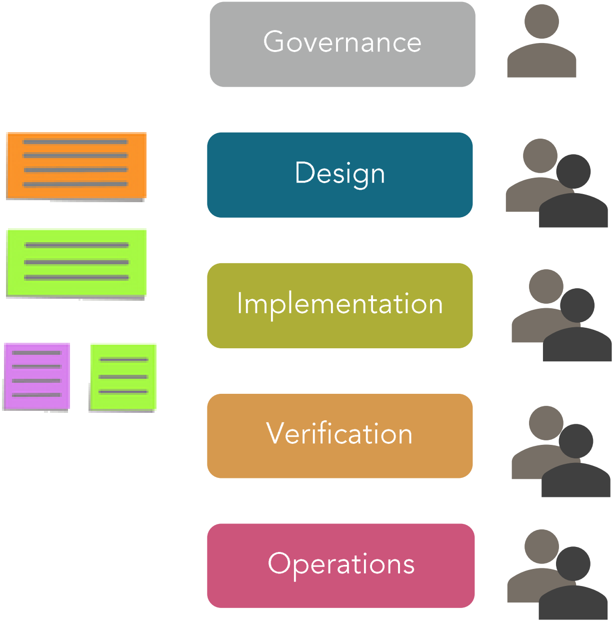
Verification

Operations





THE TEAM OWNS THE ROADMAP



NIST

DSOMM

OWASP/ASVS
Application Security Verification Standard

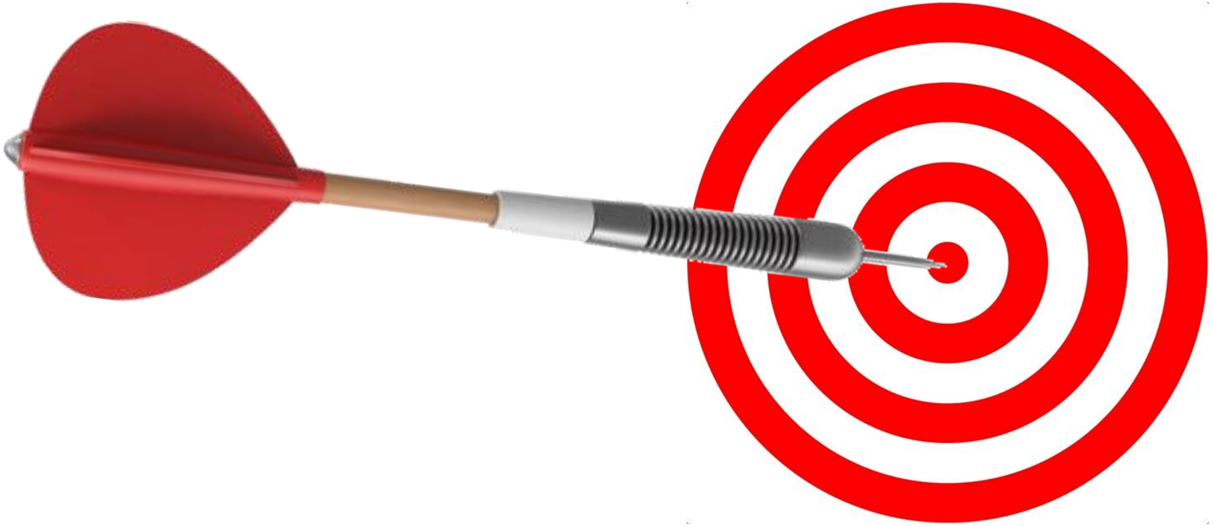
OWASP
CHEAT SHEET
SERIES PROJECT

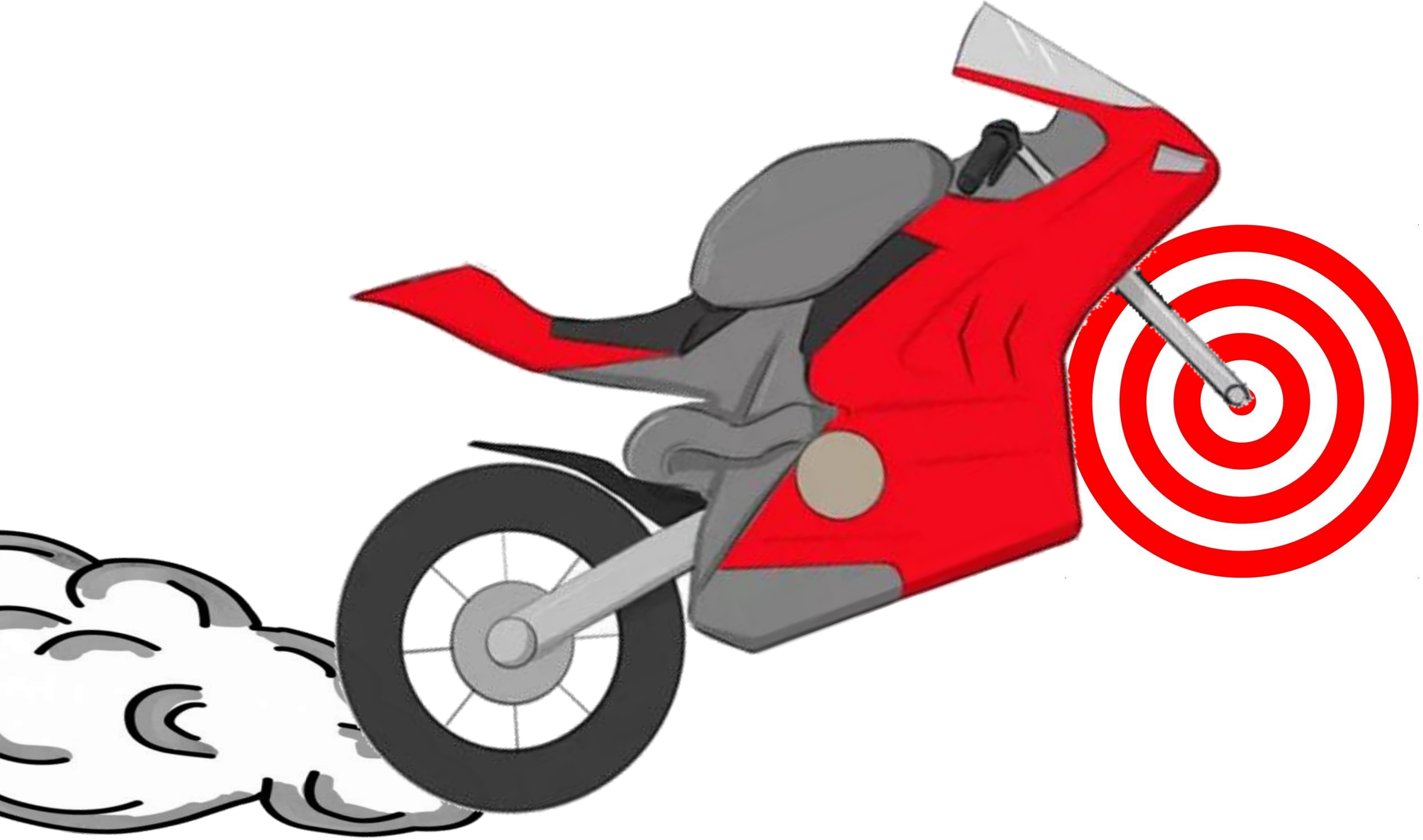
OWASP
TOP10

CIS Benchmarks™

"You get what you measure"

- Richard Hamming





Baseline score

- Your initial SAMM scores

Current score

- Your current SAMM scores

Target score

- SAMM scores that represent an acceptable level of risk
- **You should improve to reach the target, not an absolute 3.0!**

Percent to target

PercentToTarget = 1 - Gap / Target

Activity	Current	Target	Gap	Percent to target
I-SB-A-1	0.75	1.00	0.25	75%
I-SB-A-2	0.00	0.75	0.75	0%
I-SB-A-3	0.00	0.00	0.00	100%
I-SB-B-1	1.00	0.75	0.00*	100%
I-SB-B-2	0.25	0.75	0.50	33%
I-SB-B-3	0.00	0.00	0.00	100%

Legend

- Within target
- Need to improve
- “Not applicable”

* Gap is zeroed out to avoid giving credit for “overshooting”

THE TEAM OWNS THE ROADMAP

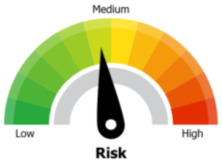
Governance

Design

Implementation

Verification

Operations



75%
0%
100%
100%
33%
100%

Initiatives

🔗

Targets

Summary

SAMM requires interpretation

Interviews work better than questionnaires

→Coaching & consistency

SAMM scores are "personal"

→Relative to the team/scope

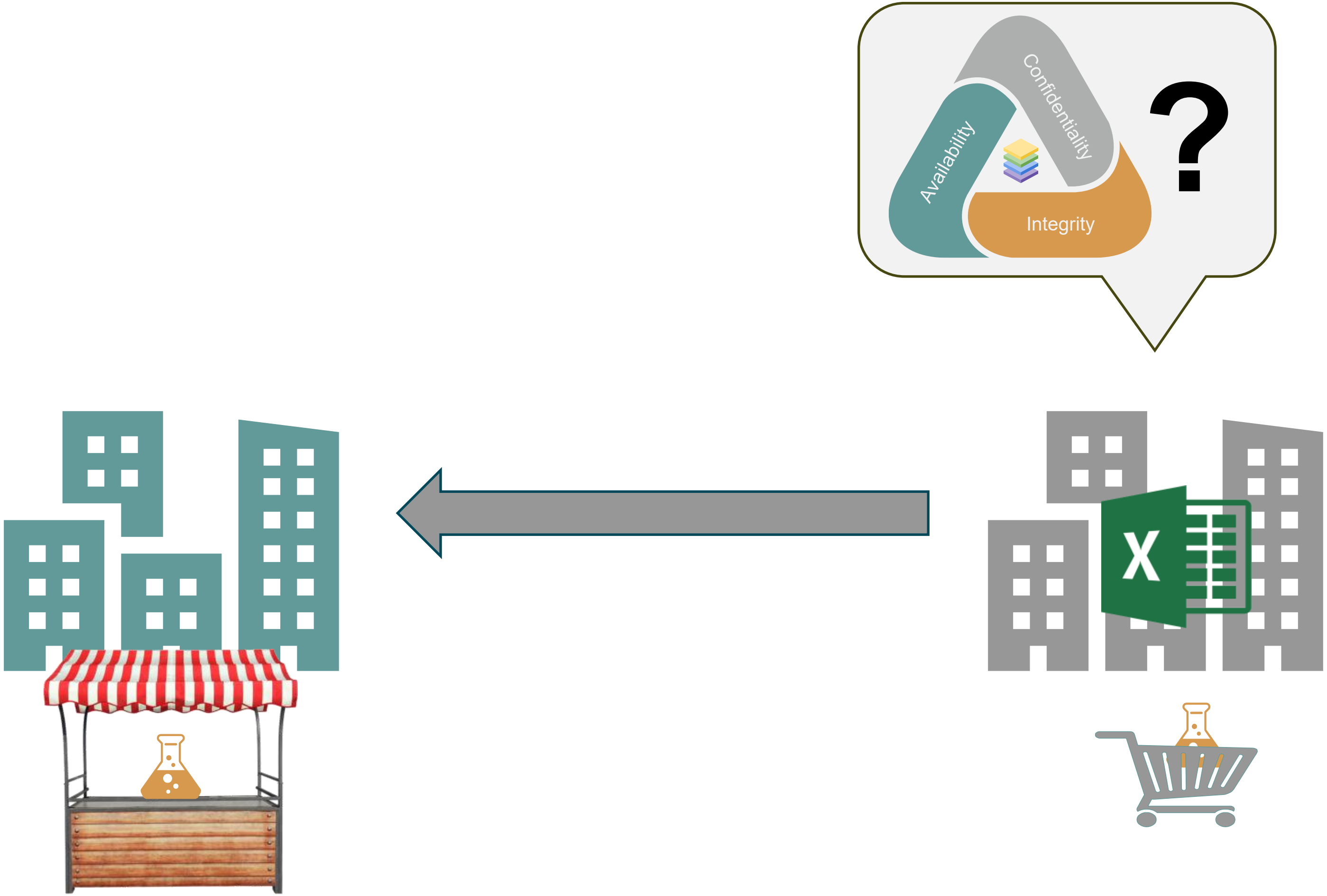
Targets are relative to the team/score AND risk

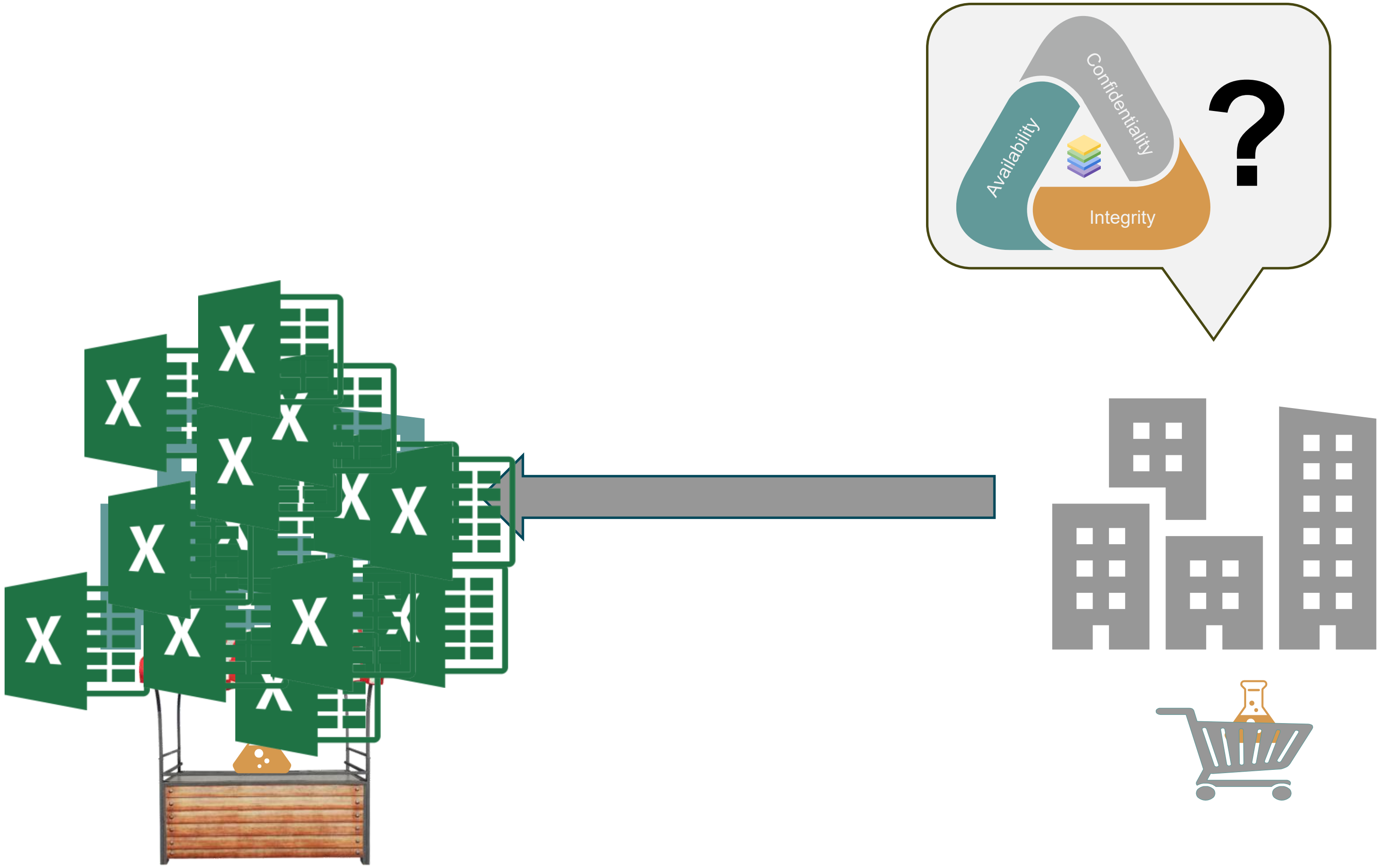
→Measure progress, not raw scores

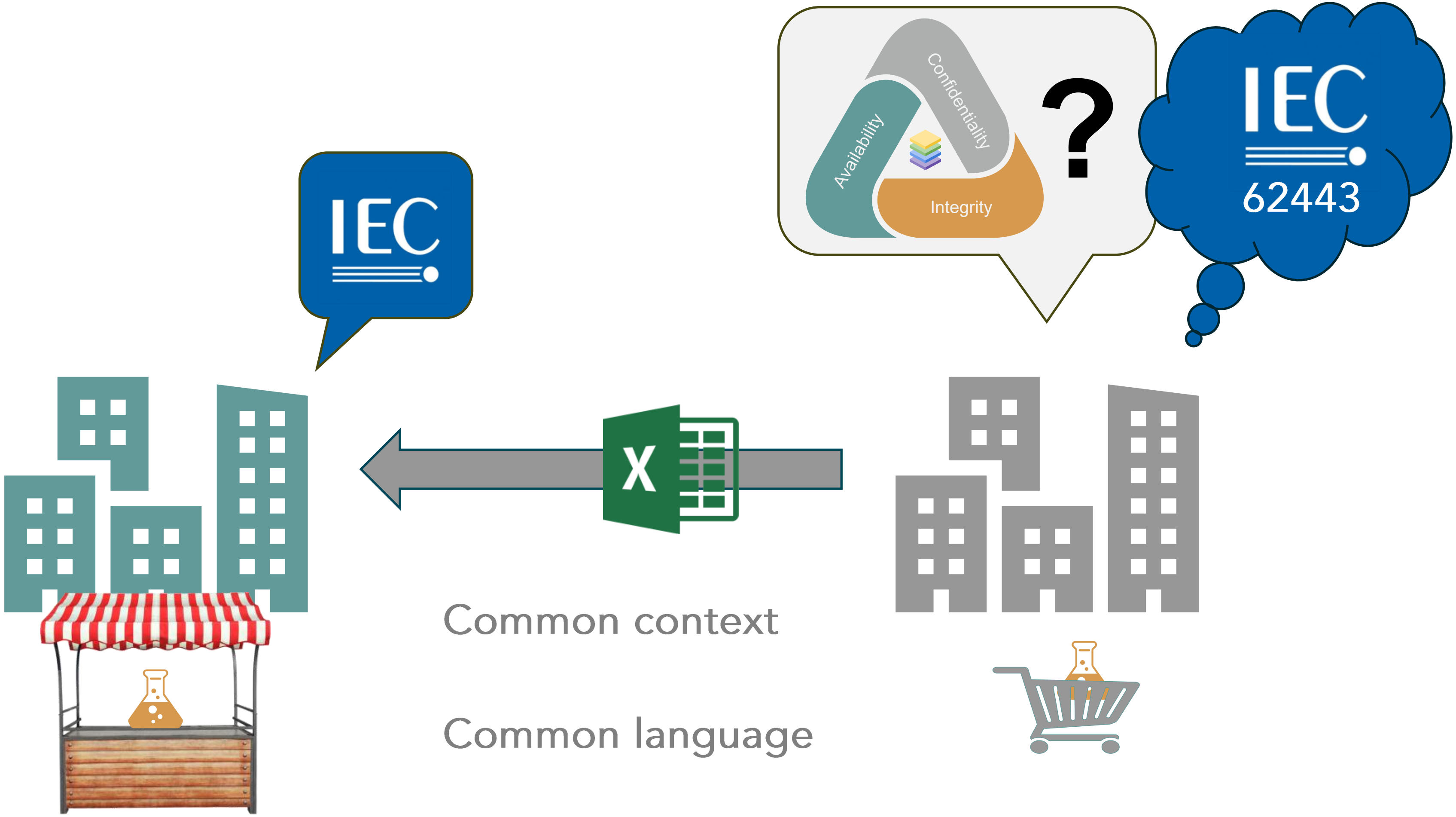
→Use initiatives to support team progress

SAMM: 12-24m

Roadmap Progress: 3-6m


Confidentiality
Availability
Integrity
?


Confidentiality
Availability
Integrity
?



Common context

Common language

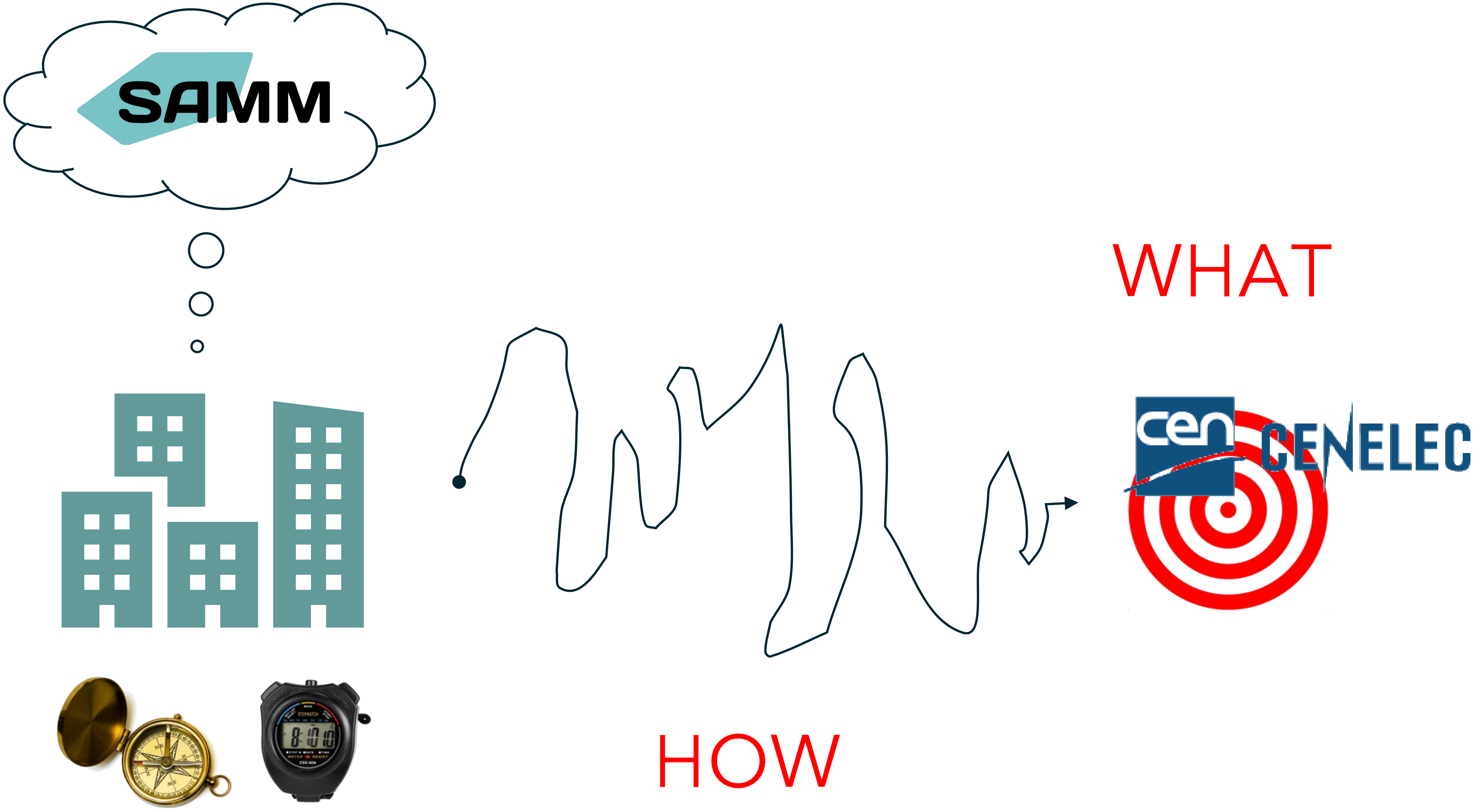
Clear delineation of shared responsibilities

WHAT

HOW

CE

Confidentiality
Availability
Integrity
?



WHAT

HOW

WHAT

HOW

SAMM & OSS

OWASP
JUICE SHOP
SecureFlag
Secure
Coding
BUILD SECURITY INTO DEVOPS
OWASP
corda campus

owaspsamm.org

github.com/owaspsamm

#project-samm

meetup.com/owaspsamm

2nd Wednesday
of the month

21:30 CET - 3:30 pm EDT/EST

2nd Friday
of the month

14:00 CET - 8:00 am EDT/EST

meetup.com/owasp-samm

Thank you