



Navigating Product security compliance

with OWASP SAMM

PRESENTED BY TOREON

Maxim Baele

Volunteer

OWASP Belgium chapter leader

OWASP SAMM core team member

OWASP EU Board Member

OWASP Regulations & Standards Liaison

→ Bridge-builder

Eclipse ORC-WG (Resources)



Maxim Baele

Principal Consultant Product Security @TOREON

Tinkering with Linux

Linux system engineering

Automation

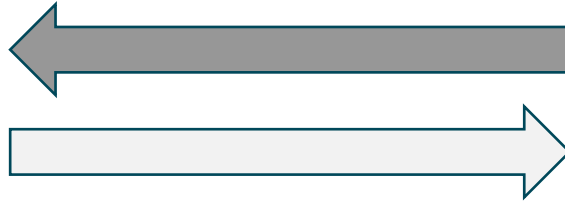
Build systems (CI/CD)

Product Security



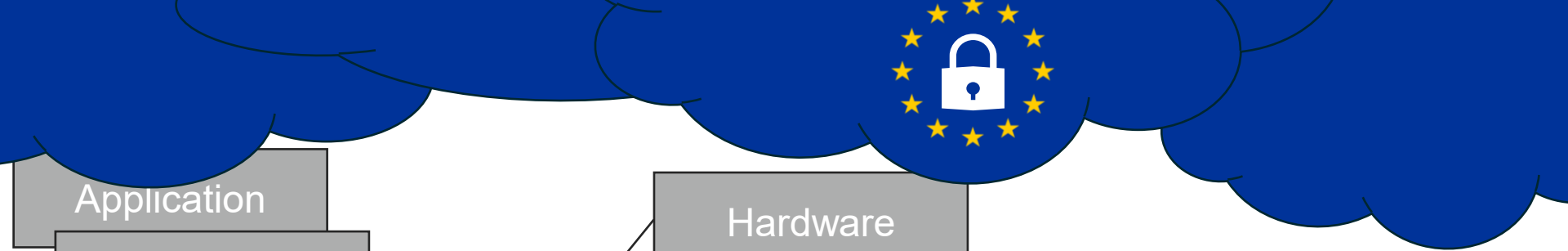


Supply Chain Security



Product Security





Application

Application

Application

Hardware

Dev & Build
Infrastructure

Hosting
Infrastructure



People &
Processes

Business
Context



New Legislative Framework (NLF)

Essential safety requirements
(or other requirements on the general interest)

...with which products put on the market must conform

...and which will therefore enjoy free movement throughout the territory of the European Union

*Products are “placed on the market” by a **manufacturer** or an **importer** when they supply a product to a **distributor** or an end-user for the first time*

Products made available on the market must comply with the applicable Union harmonisation legislation at the moment of placing on the market.

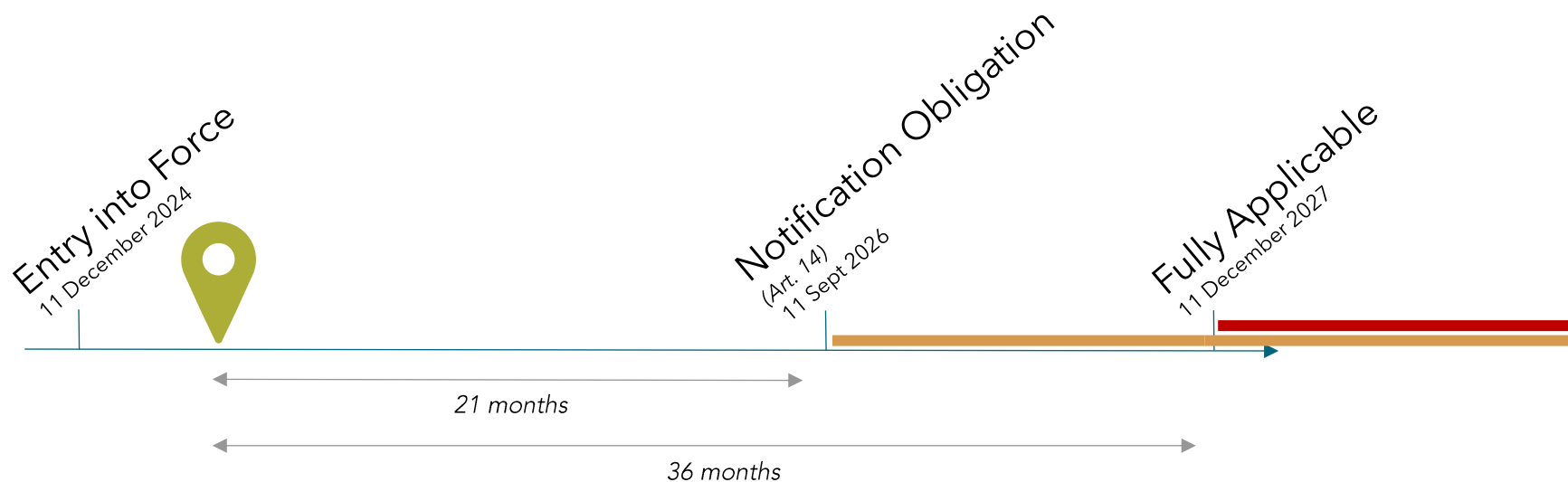




Cyber Resilience Act (CRA)

Adds essential *cybersecurity* requirements

...with which "*products with digital elements*" put on the market must conform





The image shows the entrance to a bookstore. The 'finac' logo is prominently displayed in large, white, 3D letters above the entrance. To the right, the 'Vanden Born' logo is visible in red, 3D letters. The interior of the store is visible through the entrance, showing bookshelves and promotional displays. On the left, there is a large poster for 'PRINT JE TOEGANG' and a sign for 'Print je foto's direct vanaf je smartphone'. In the foreground, several tall, narrow promotional displays are visible, each featuring a '-10%' discount sign and images of books. The ceiling is made of white, horizontal slats, and the floor is a light-colored carpet.

finac

Vanden Born

NOT:

- "Pure" SaaS
- Subject to more specific legislation
Medical devices, cars, aerospace, ...
- Non-commercially supported
Open Source Software

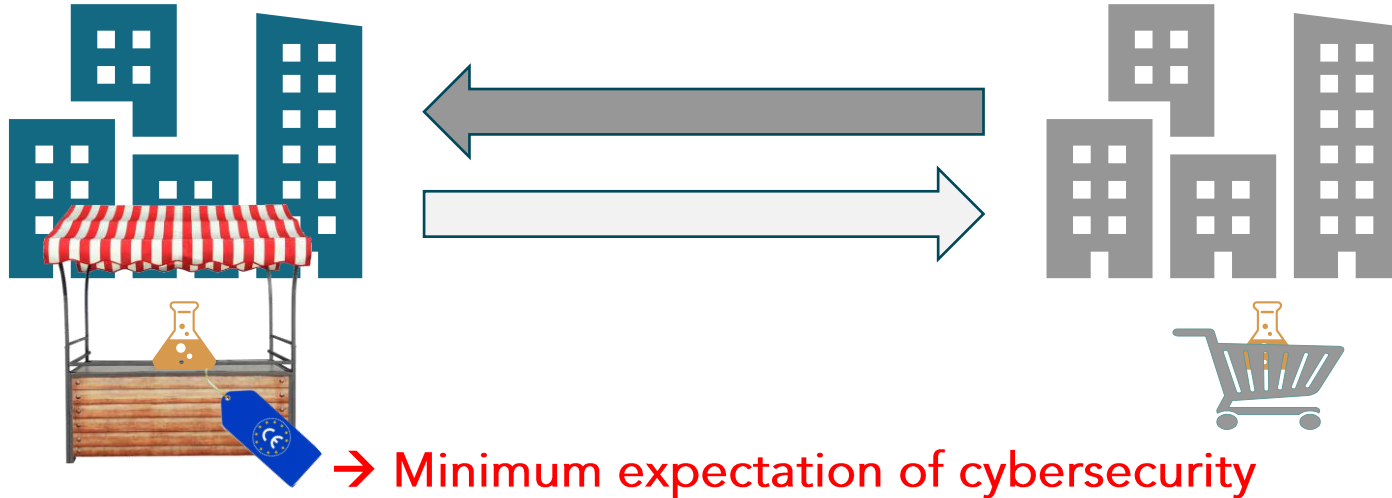
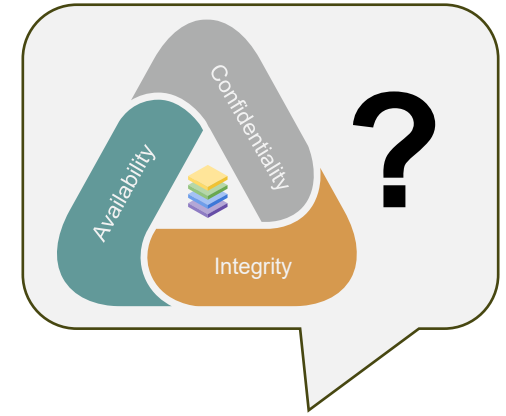
Secure by design, based on risk analysis

Released without known, exploitable vulnerabilities

Adhering to high-level Technical Requirements

Patchable

Vulnerability handling



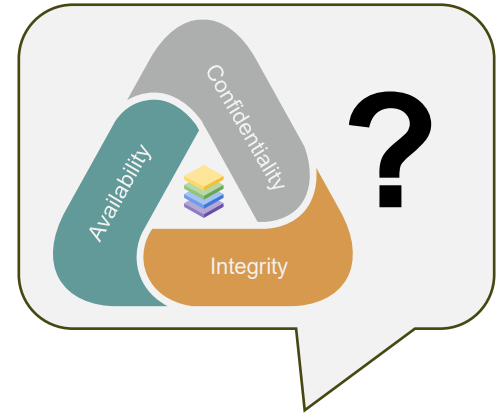
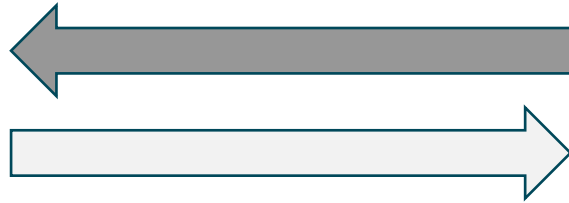
Governance

Design

Implementation

Verification

Operations

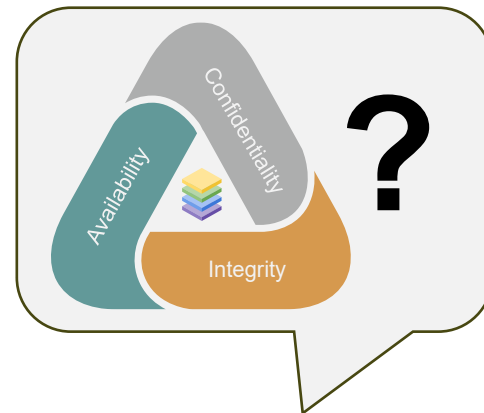


Governance

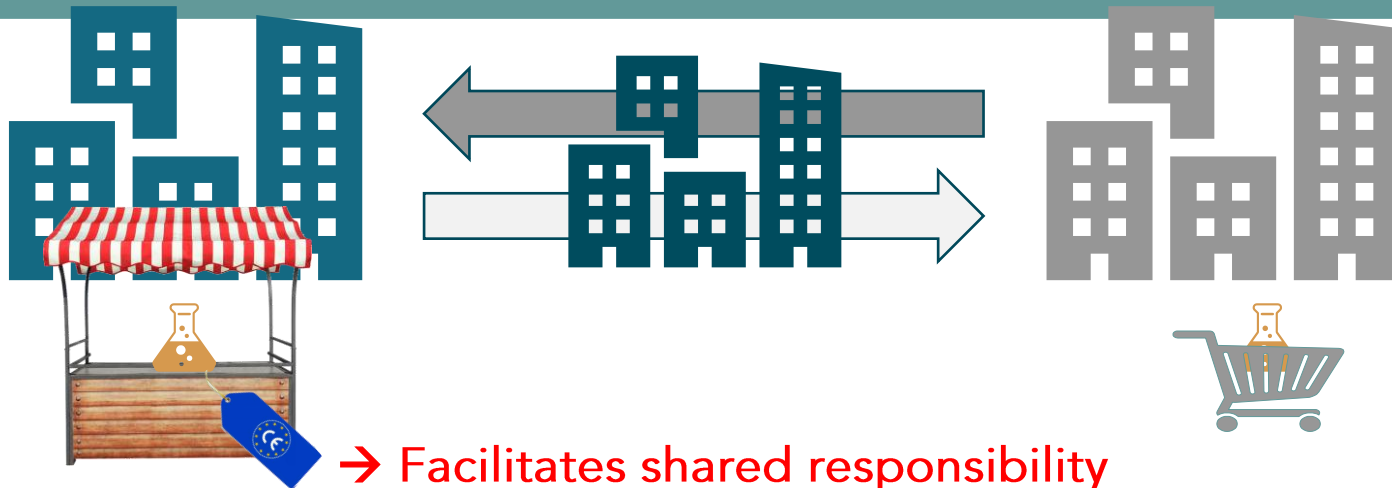
Design

Implementation

Verification



Operations



→ Facilitates shared responsibility



Operations

OPERATION

WARNING:

Battery tools are always in operating condition. Therefore, switch should always be locked when not in use or carrying at your side.

KICKBACK

See Figures 6 - 9.

Kickback occurs when the blade stalls rapidly and the saw is driven back towards you. Blade stalling is caused by any action which pinches the blade in the wood.

DANGER:

Release switch immediately if blade binds or saw stalls. Kickback could cause you to lose control of the saw. Loss of control can lead to serious injury.

To guard against kickback, avoid dangerous practices such as the following.

- Setting blade depth incorrectly.
 - Sawing into knots or nails in workpiece.
 - Twisting the blade while making a cut.
 - Making a cut with a dull, gummed up, or improperly set blade.
 - Supporting the workpiece incorrectly.
 - Forcing a cut.
 - Cutting warped or wet lumber.
 - Operating the tool incorrectly or misusing the tool.
- To lessen the chance of kickback, follow these safety practices.
- Keep the blade at the correct depth setting. The depth setting should not exceed 1/4 in. below the material being cut.
 - Inspect the workpiece for knots or nails before cutting. Never saw into a knot or nail.
 - Make straight cuts. Always use a straight edge guide when rip cutting. This helps prevent twisting the blade.
 - Use clean, sharp, and properly set blades. Never make cuts with dull blades.
 - Support the workpiece properly before beginning a cut.
 - Use steady, even pressure when making a cut. Never force a cut.
 - Do not cut warped or wet lumber.
 - Hold the saw firmly with both hands and keep your body in a balanced position so as to resist the forces if kickback should occur.

WARNING:

When using the saw, always stay alert and exercise control. Do not remove the saw from the workpiece while the blade is moving.

KICKBACK - BLADE SET TOO DEEP

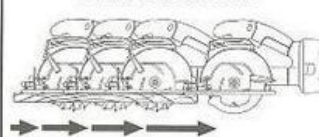
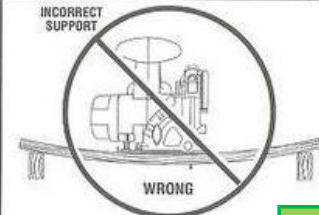
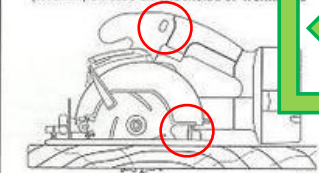


Fig. 6

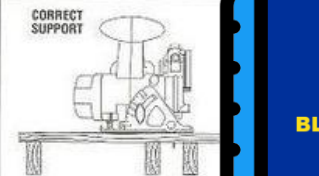
INCORRECT SUPPORT



CORRECT BLADE DEPTH SETTING - BLADE EXPOSED 1/4 in. (6.35 mm) OR LESS ON UNDERSIDE OF WORKPIECE



CORRECT SUPPORT



BLUE GUIDE



→ Presumption of Conformity



Entry into Force
11 December 2024



Notification Obligation
(Art. 14)
11 Sept 2026

Fully Applicable
11 December 2027

Vulnerability Handling
Standard
30/08/2026

Critical Product
Standards
30/10/2026

Requirements
Standards
30/10/2027



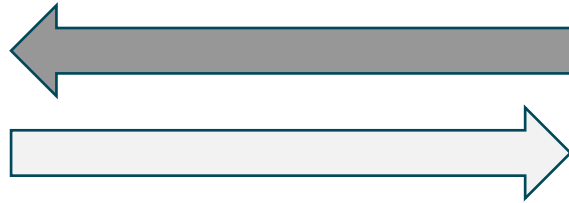
Governance

Design

Implementation

Verification

Operations



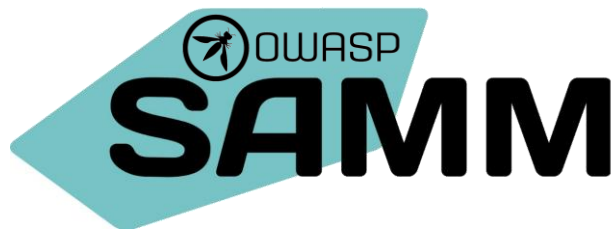
Governance

Design

Implementation

Verification

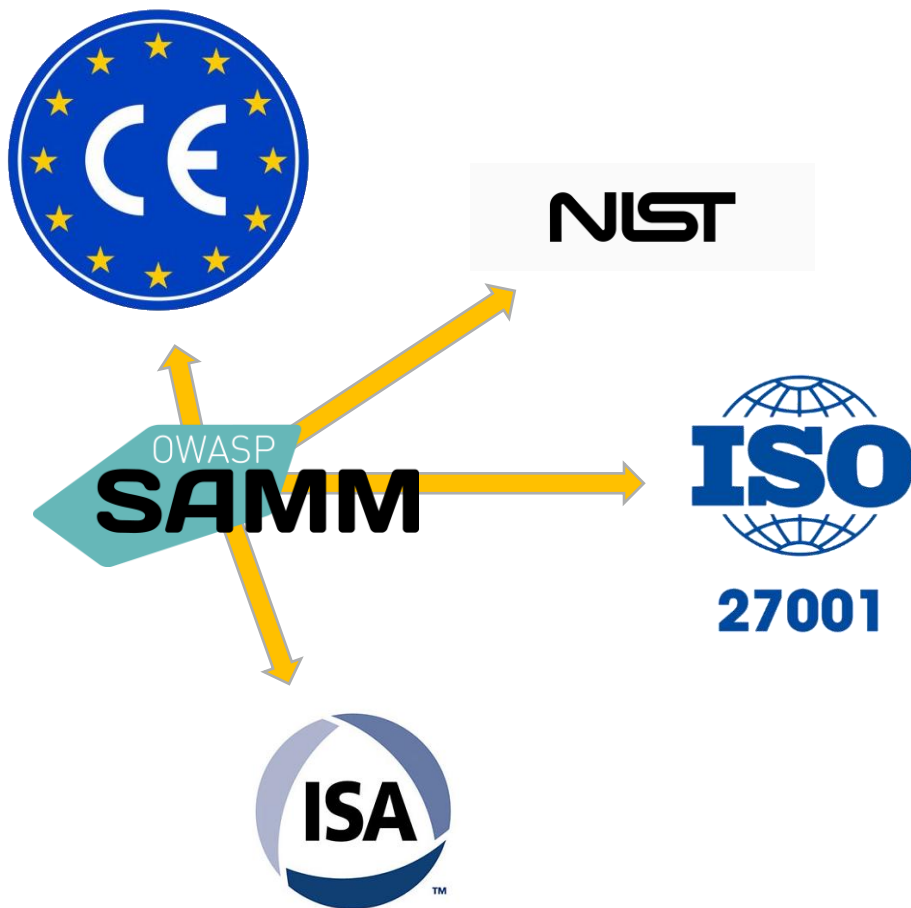
Operations



Software Assurance Maturity Model

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

<https://owaspsamm.org>



- 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
- ?



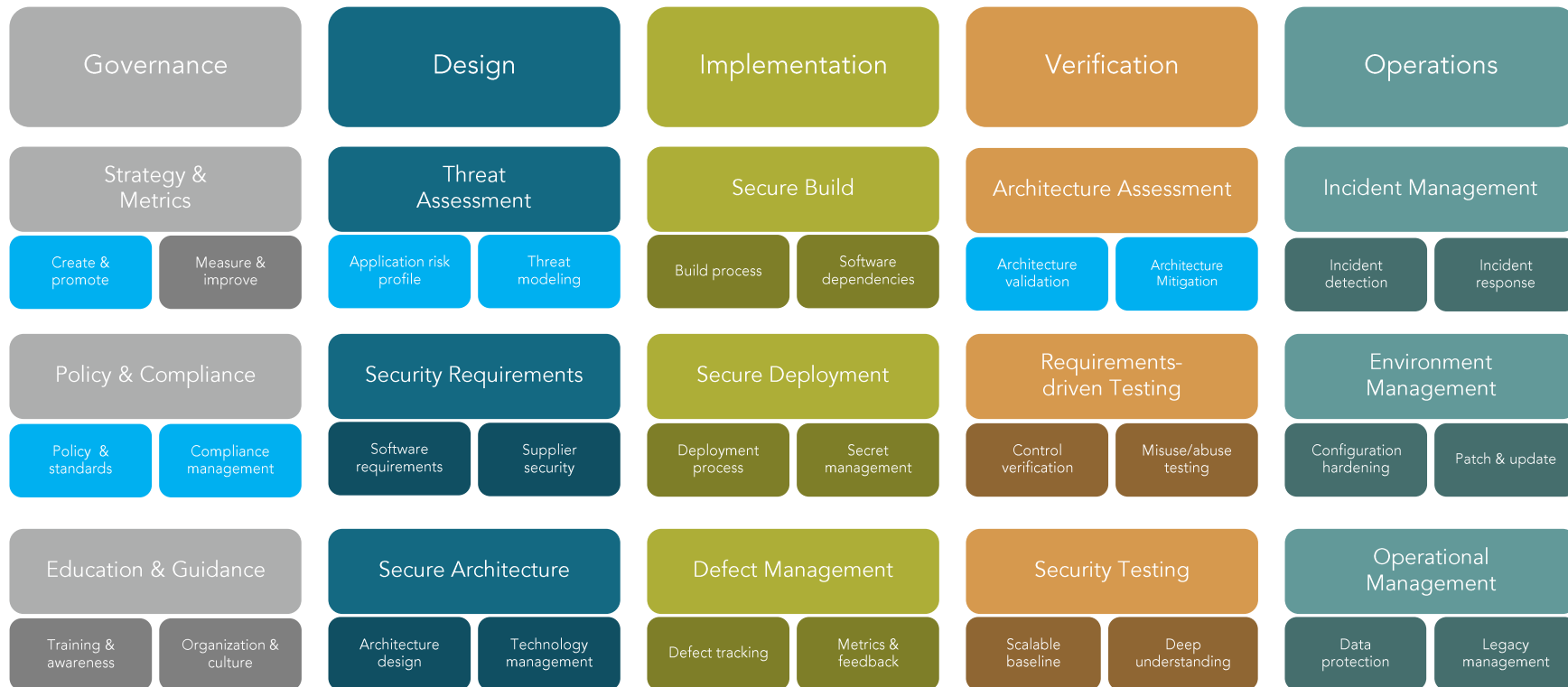
Secure Development Lifecycle

Secure by design, based on risk analysis

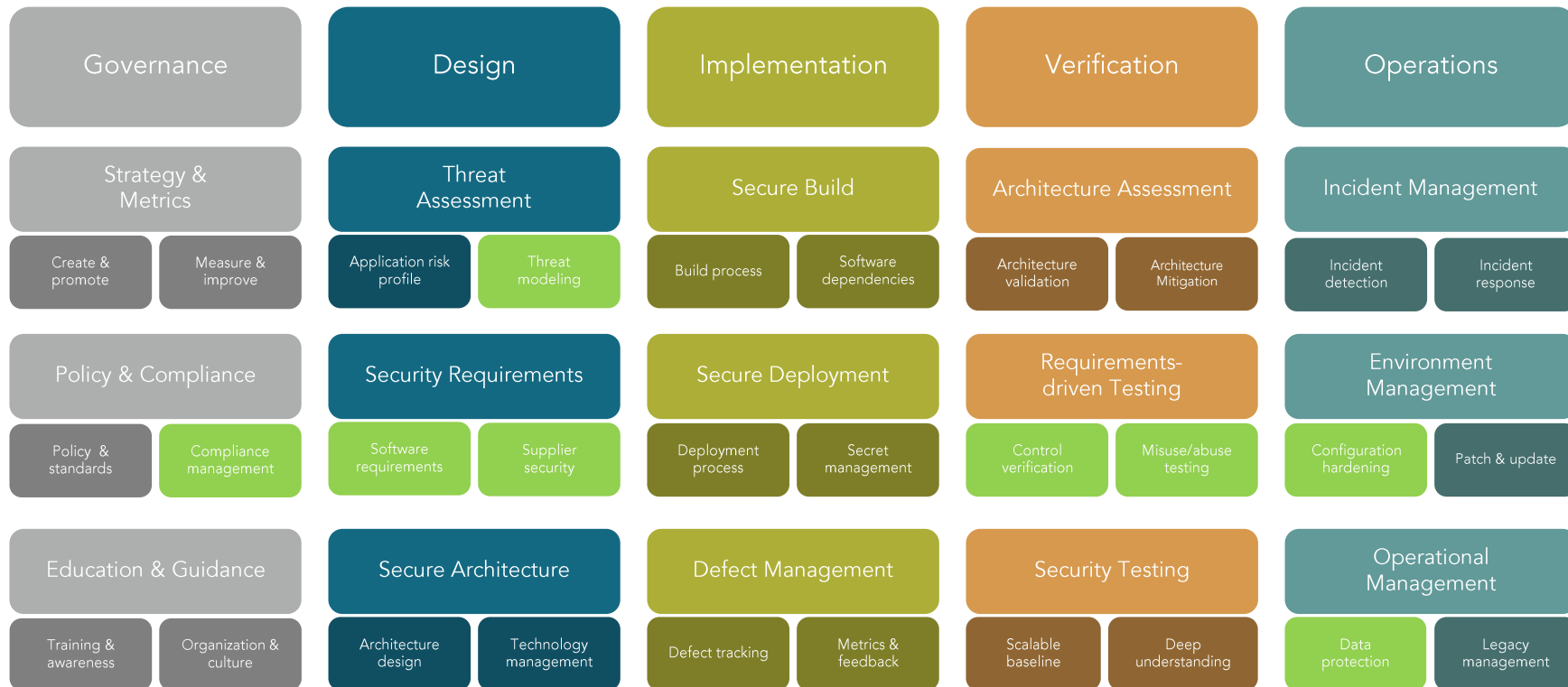
Released without known, exploitable vulnerabilities
Adhering to high-level Technical Requirements
Patchable

Vulnerability handling

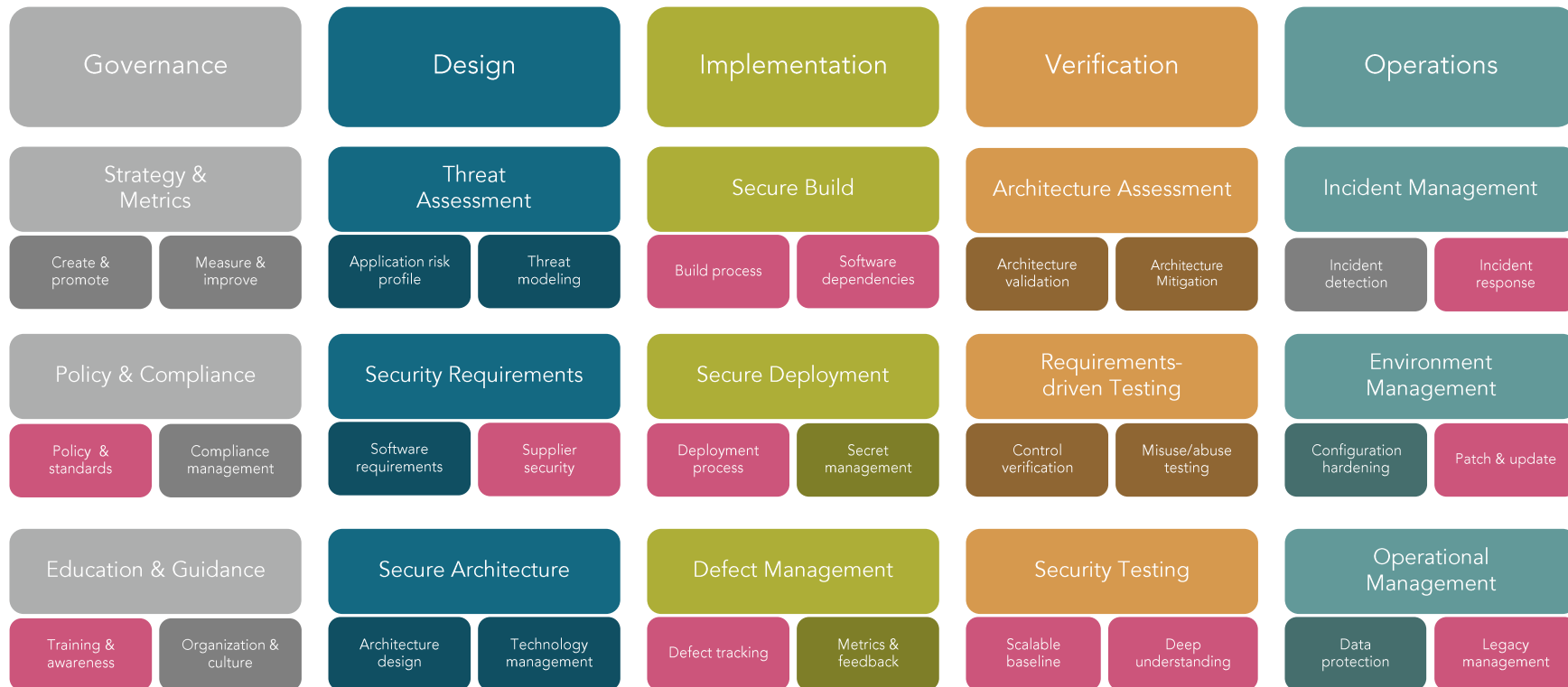
Secure by design, based on risk analysis



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



Vulnerability handling

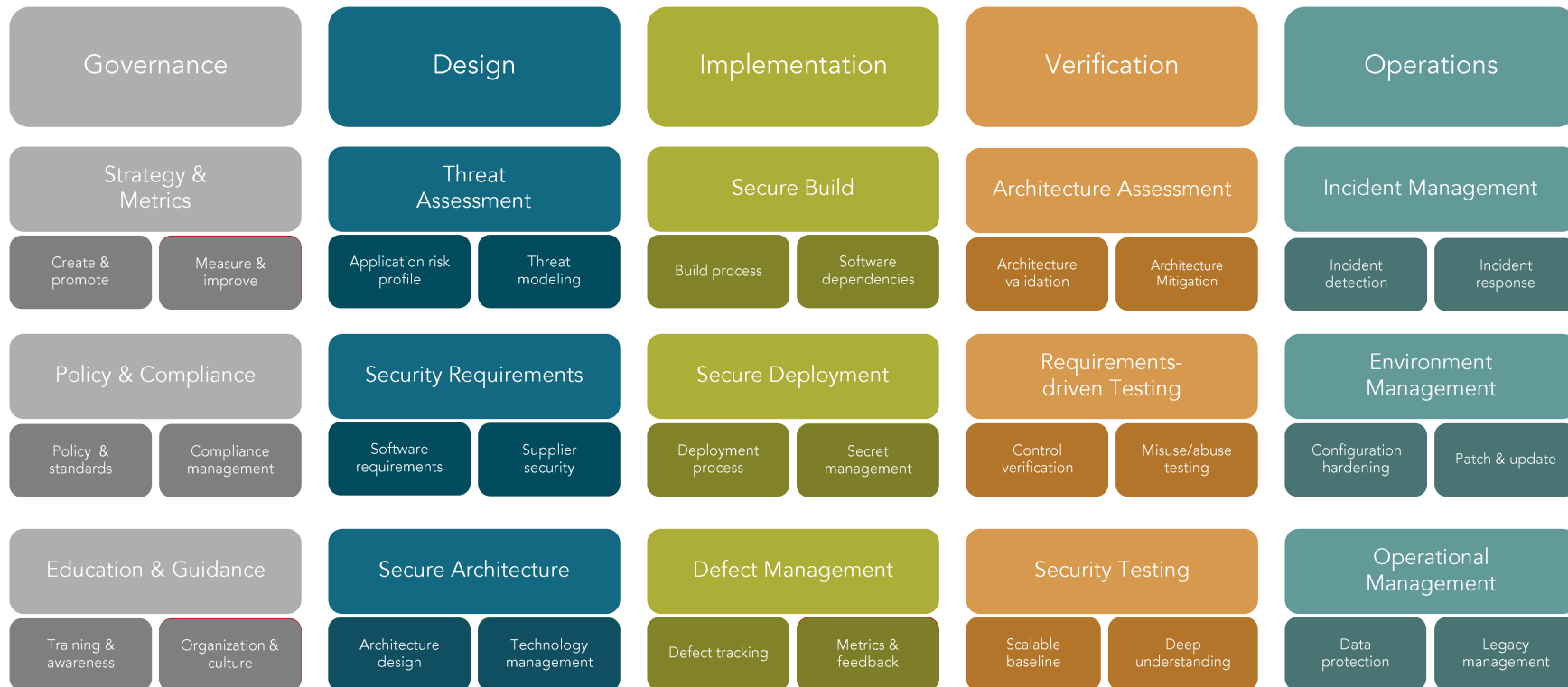


Do you classify applications according to business risk based on a simple and predefined set of questions?

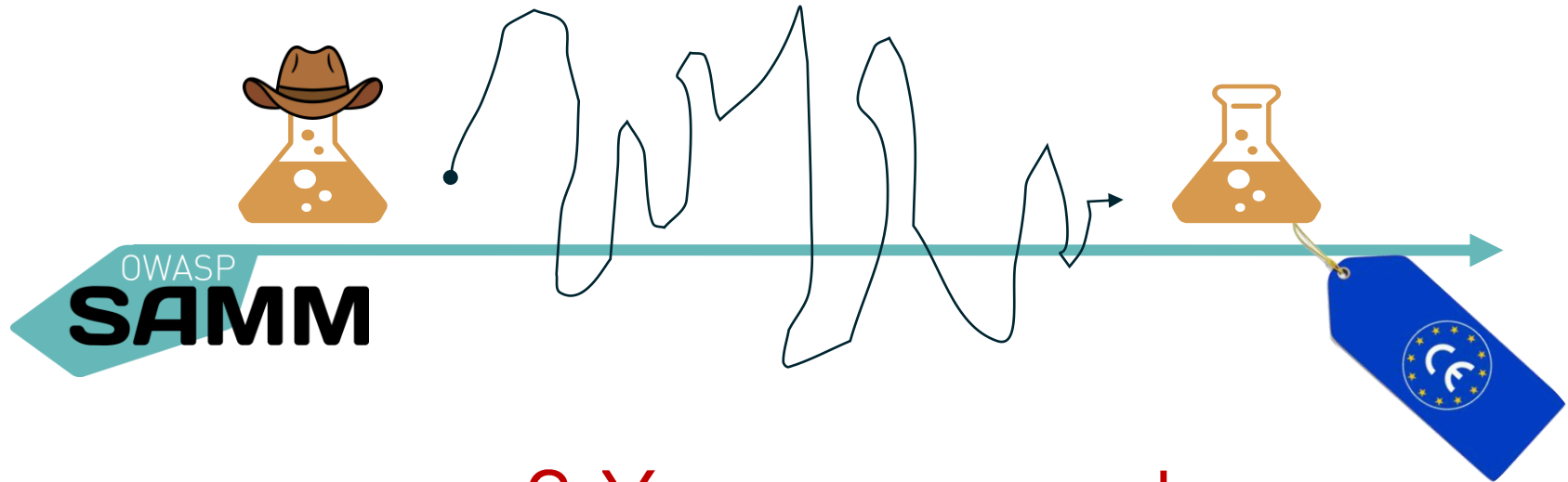
An agreed-upon risk classification exists	Yes	A clear and simple risk classification system is in place, at minimum aligning with CRA product classification categories. All products are classified, including existing and legacy applications.
The application team understands the risk classification	Yes	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-compliances 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"

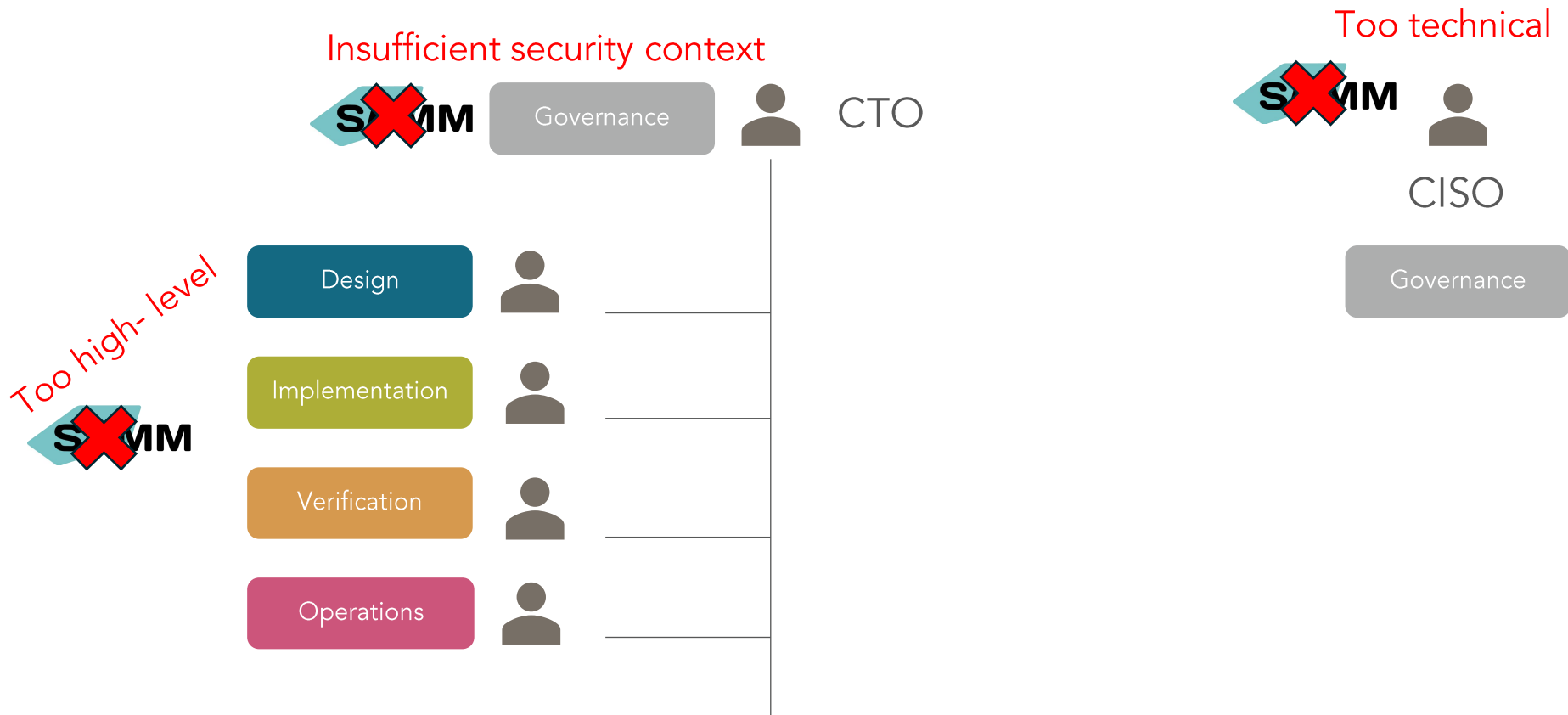


→ Product Security Strategy



>2 Year journey!

Who Owns Product Security Strategy?

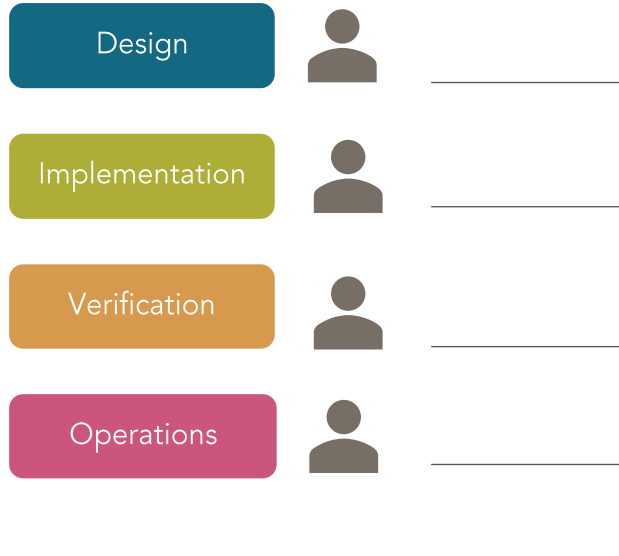


Who Owns Product Security Strategy?

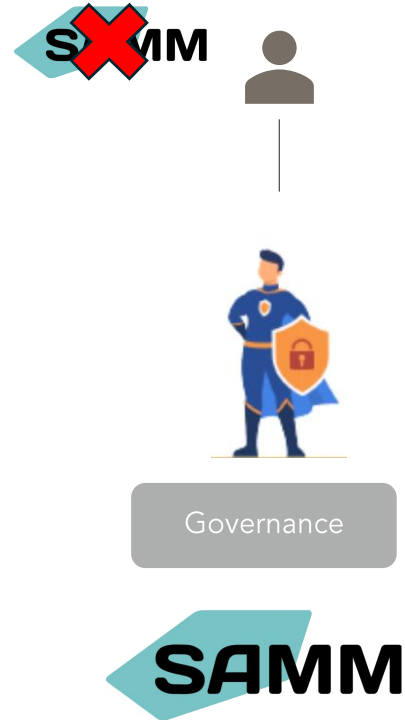
Insufficient security context



Too high-level



Too technical



Who Owns Product Security Strategy?

Technical background

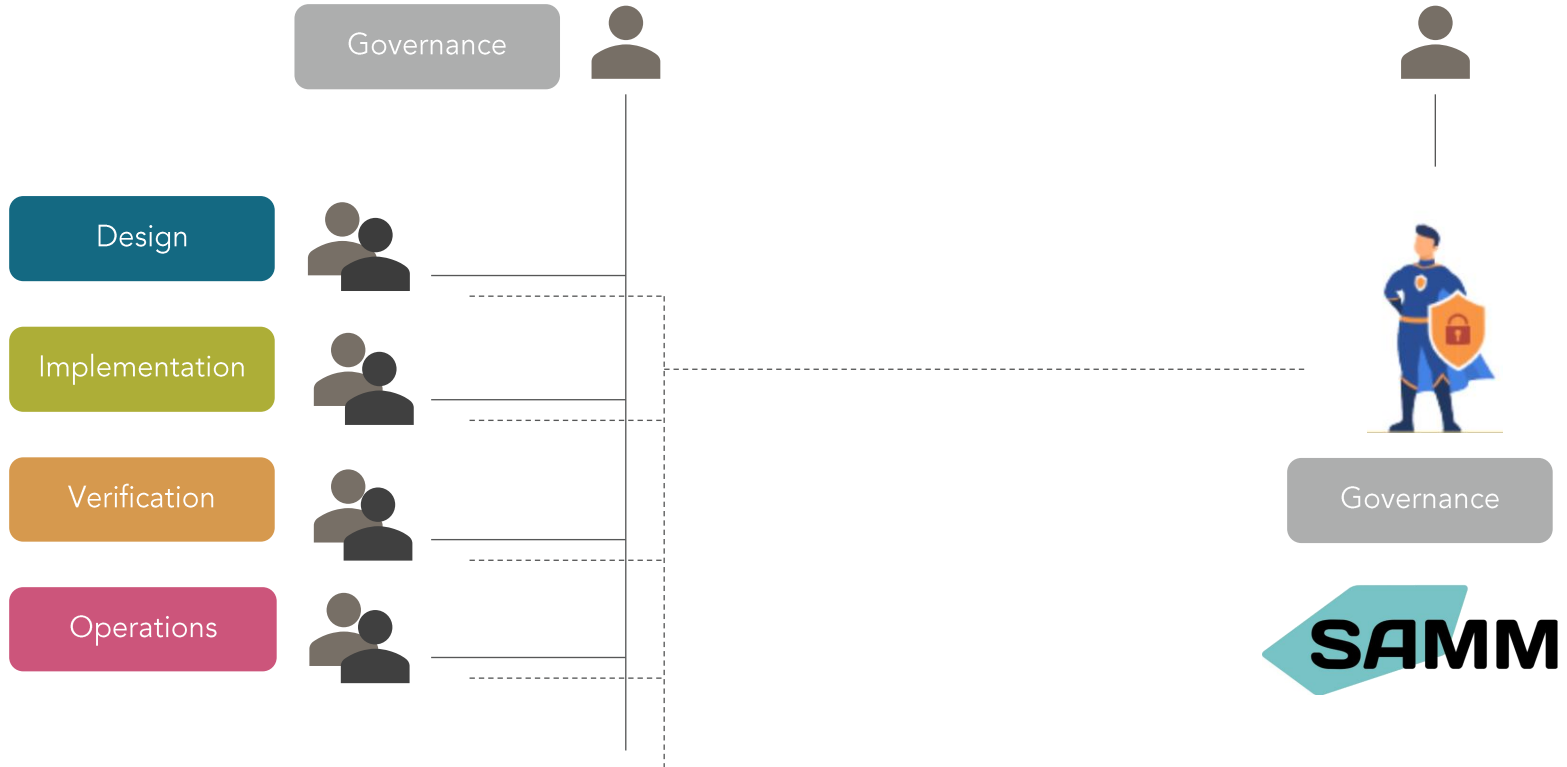
CTO, Architect, Lead Developer

Security Champion

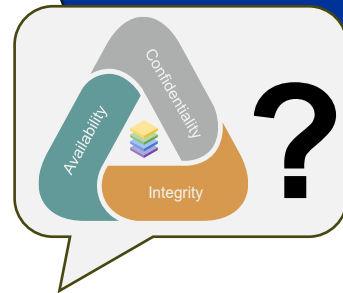
- Advisory role!
- Assistance from legal
- Supported by the full organization



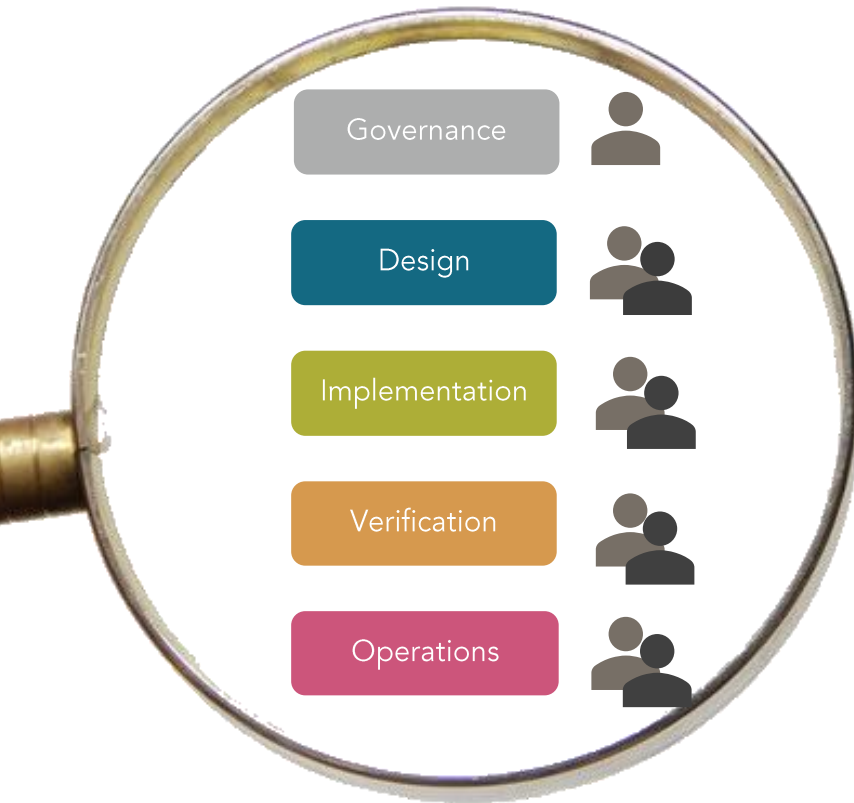
Who Owns Product Security?



SAMM



SAMM



Focused on a single product
...or similar set of products

Taking part in the same SDLC



Scope

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

Governance



Design



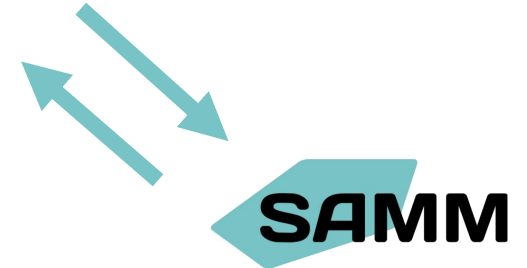
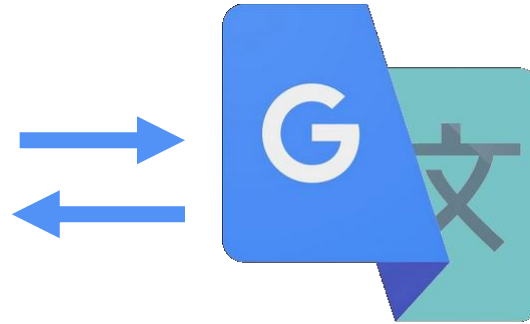
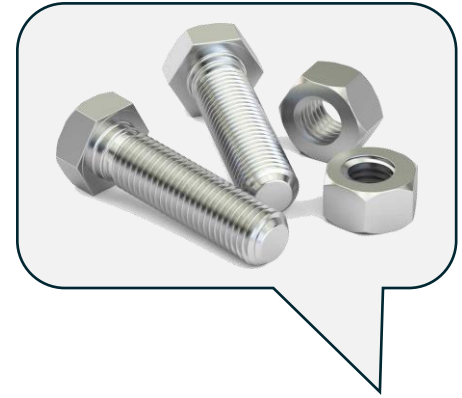
Implementation



Verification



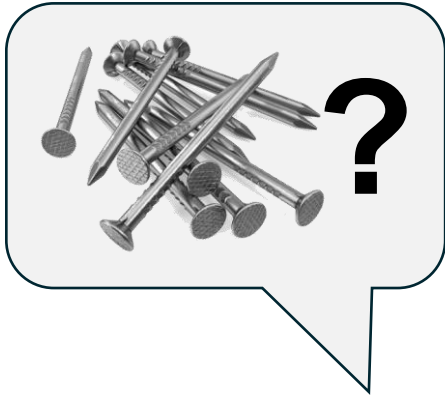
Operations



Governance



Design



Implementation



Verification

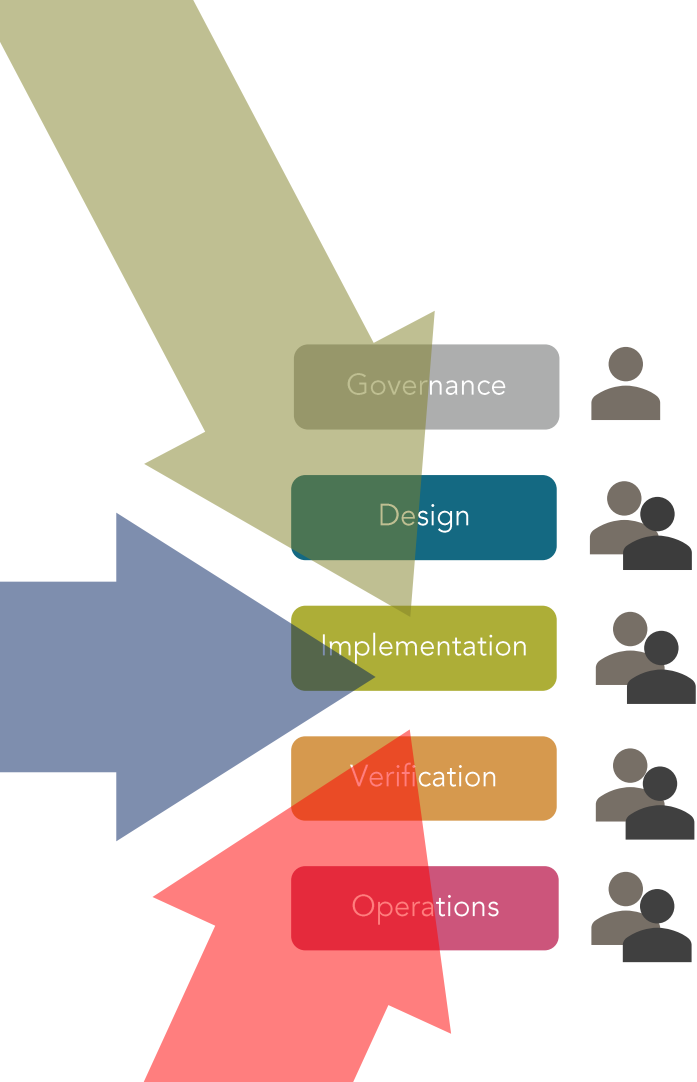


Operations



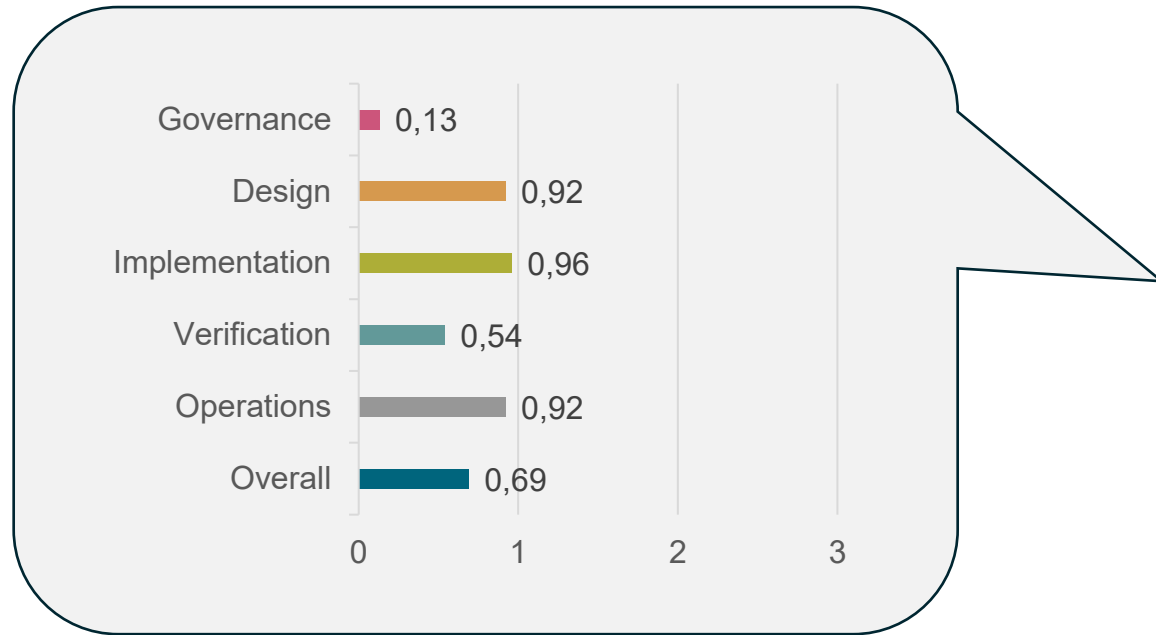
Security Testing	
1	Do you scan applications with automated security testing tools?
You dynamically generate inputs for security tests using automated tools	
You choose the security testing tools to fit the organization's architecture and technology stack, and balance depth and accuracy of inspection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





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

SCORES ARE RELATIVE



SCORES ARE RELATIVE

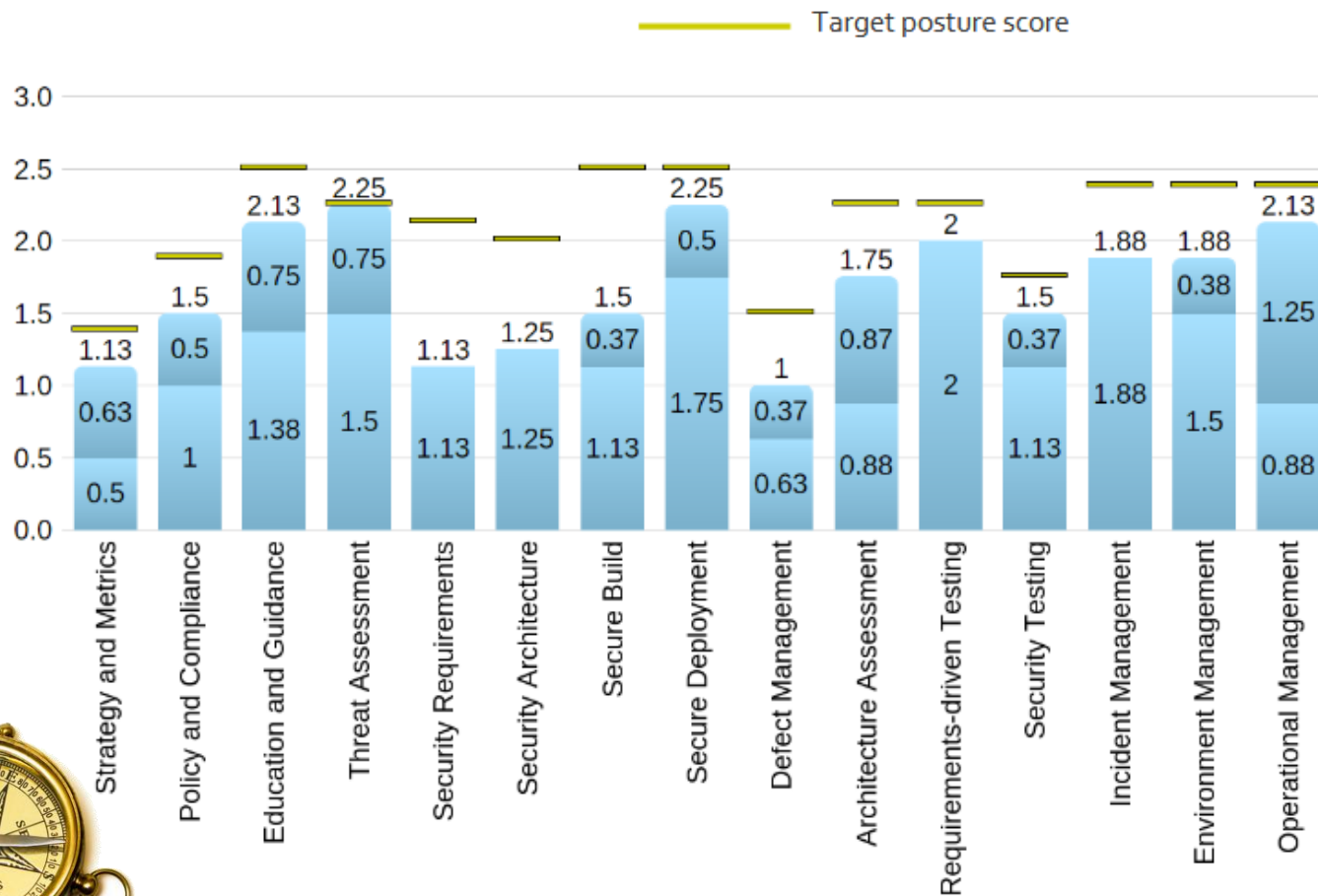
- ...to the organization's risk appetite
- ...to the team's maturity
- ...to a point in time
- ...to the assessor (in some cases)

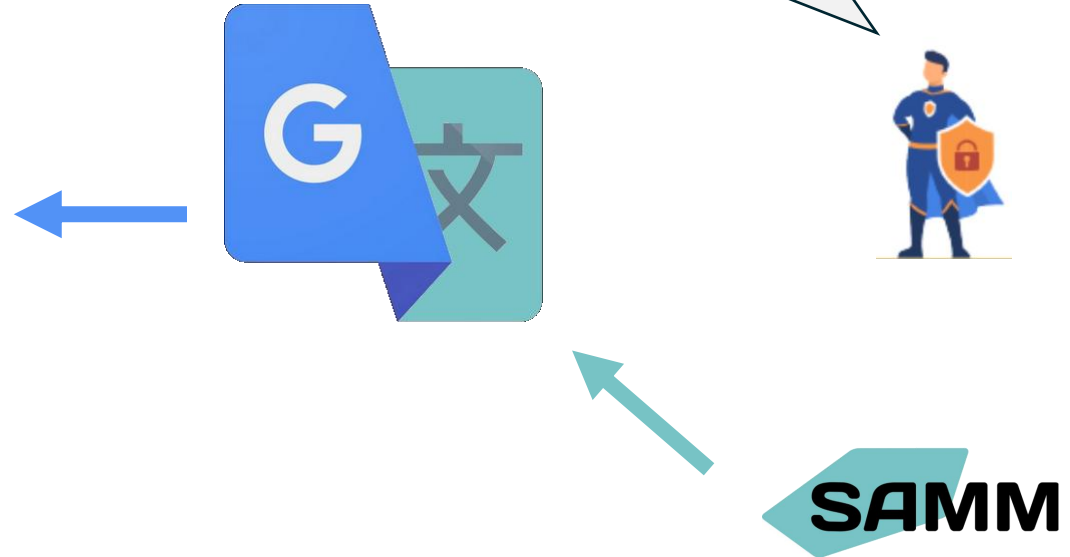
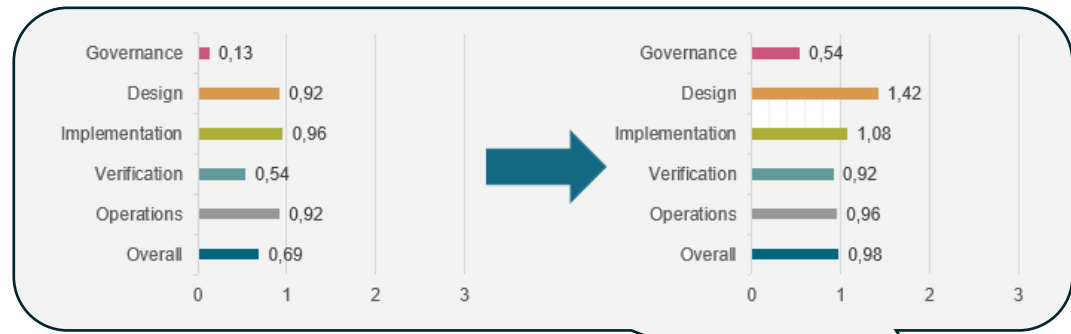
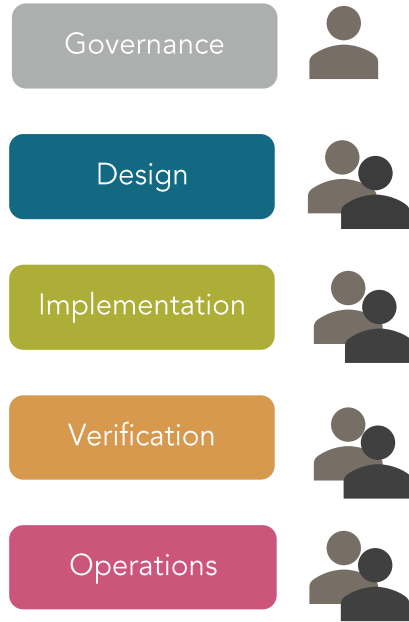
TARGETS ARE RELATIVE

- ...to the capacity for change
- ...to market and legislative demands
- ...to the lifecycle of the product(s) in scope



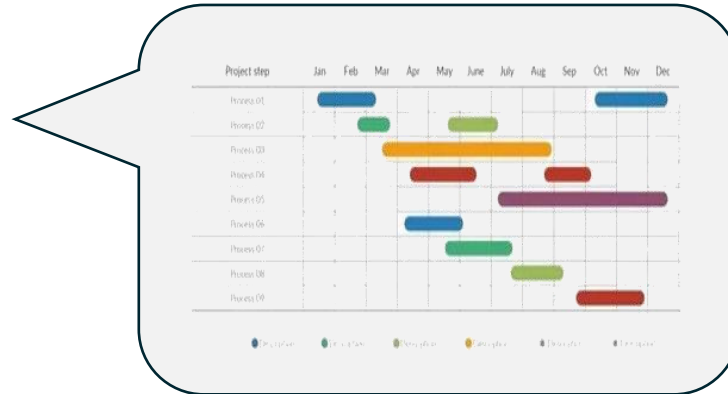
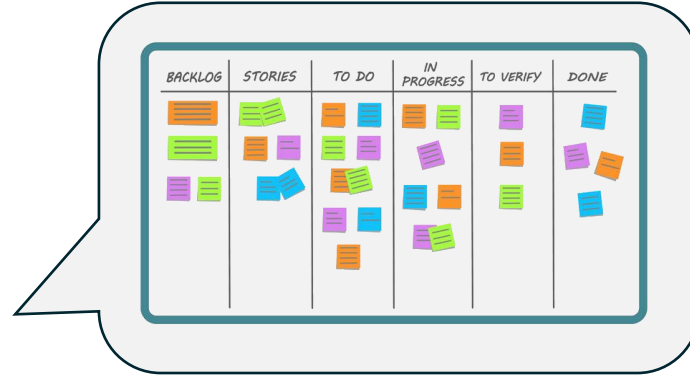
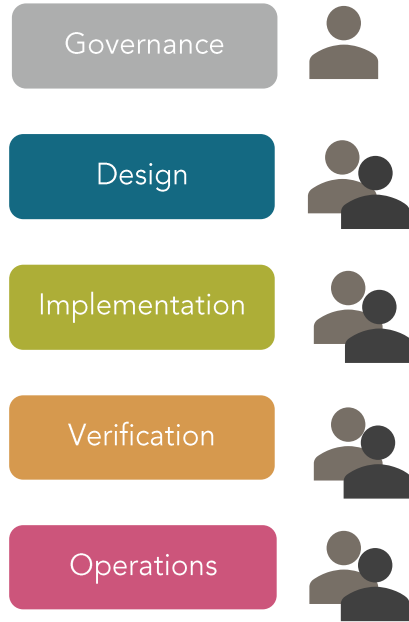
Per practice





THE TEAM OWNS THE ROADMAP





Too high-level
Scrum

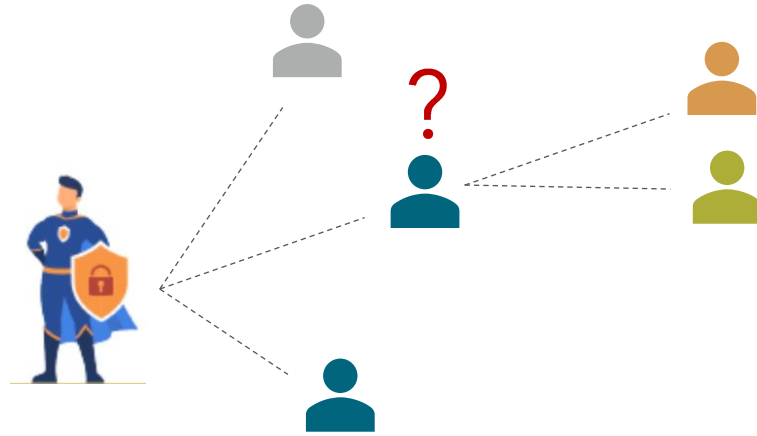


THE TEAM OWNS THE ROADMAP



→ <https://owaspsamm.org/blog/2025/02/09/owasp-samm-skills-framework>

Stream	Stream Goal	Leading Assignment	Stakeholder	Stakeholder 2	Stakeholder 3	Rationale
Application Risk Profile	Best-effort identification of high-level threats to the organization and individual projects.	Product security strategy 	Organizational Security Strategy 	Product ownership 	Architecture 	Product security strategy takes the lead, collaborating closely with Organizational Security. The latter defines the overall risk strategy and is aware of the risk appetite / tolerance of the organization. Product Ownership assists with determining the profiles and mapping risk profiles to requirements. The architecture Assignment assists with technical guidance.
Threat Modeling	Best-effort identification of high-level threats to the organization and individual projects.	Architecture	Offensive Security Testing	Product ownership	Technical Leadership (Dev Lead)	Architecture is in the lead to build out and scale the threat modeling practice. Offensive Security Testing plays an essential role coming up with realistic threat scenarios. Product Ownership helps define the threat risk. Finally, Technical leadership plays a supporting role.



Architecture

The assignment is to oversee the overall structure of systems or projects, ensuring that technical solutions align with business objectives and requirements.

Security can be a specialization in (system) architecture, but most often it needs to be considered together with the other "ilities" by every architect.

Examples of roles with this assignment:

- Product Security Architect
- Architect
- Lead Developer

[EU Cybersecurity Skills Framework](#): Cybersecurity Architect

Security Skills

- Security architecture
- Security standards
- Threat modeling

Security Training Resources

- [NIST - Engineering Trustworthy Secure Systems](#)
- [SANS SEC530 - Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise](#)
- Various applicable standards (ETSI / IEC / NIST..)
eg. NIST SP800 series, IEC62443-4-2, ETSI 303645
- [OWASP ASVS](#)

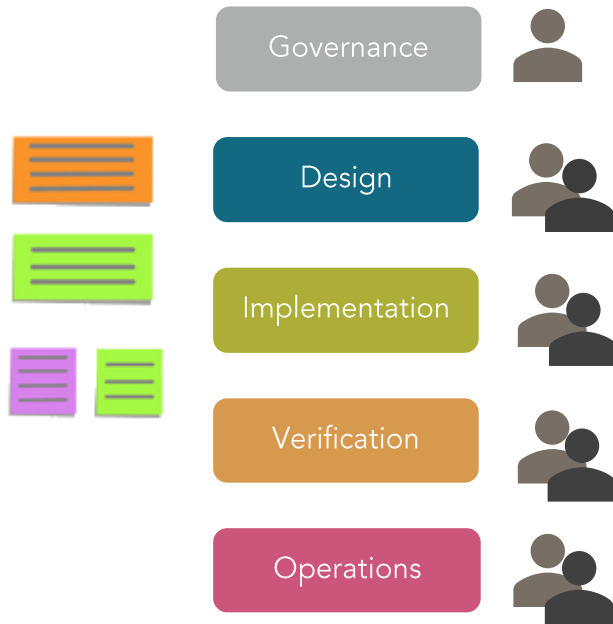
Books

- Security Engineering: A Guide to Building Dependable Distributed Systems (ISBN 9780470068526)
- Threat Modeling: Designing for Security (ISBN 9781118809993)
- Threat Modeling: A Practical Guide for Development Teams (ISBN 9781492056553)

Relevant Security Certifications

- [Paul Jerimy's Certification roadmap](#), domain "Security Architecture and Engineering"
- (ISC)² – CISSP-ISSAP (Information Systems Security Architecture Professional)
- TOGAF - Integrating Risk and Security within a TOGAF Enterprise Architecture
- SABSA - Chartered Security Architect – Foundation Certificate (SCF)
- IEC62443 Cybersecurity Expert

THE TEAM OWNS THE ROADMAP



NIST

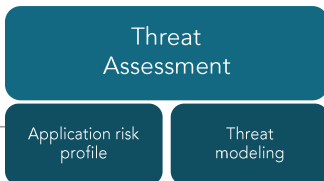




Core Team Guidance

D-TA-B

[Design | Threat Assessment](#)
[Stream B - Threat Modeling](#)



OWASP Projects and References

[OpenCRE 068-102 for references and related topics](#)

Tags

#MaturityLevel1 #MaturityLevel2 #MaturityLevel3

[OWASP Threat Dragon](#)

Rationale

Threat modeling tools are an essential part of the TM process.

Description

OWASP Threat Dragon is a modeling tool used to create threat model diagrams as part of a secure development lifecycle. Threat Dragon follows the values and principles of the threat modeling manifesto. It can be used to record possible threats and decide on their mitigations, as well as giving a visual indication of the threat model components and threat surfaces. Threat Dragon runs either as a web application or a desktop application. Threat Dragon supports STRIDE / LINDDUN / CIA, provides modeling diagrams and implements a rule engine to auto-generate threats and their mitigations.



Community Guidance

D-TA-B

[Design | Threat Assessment](#)
[Stream B - Threat Modeling](#)

Best Practices

[Pragmatic threat modeling process and outcome](#)

Rationale

Having a practical threat modeling approach is essential for this practice.



Description

Here is what works well for our organization in the context of a pragmatic threat modeling process.

- All stakeholders involved in SDLC have taken at least a basic training on threat modeling. This includes not only the architects and security savvy team members, but especially all devs and QA. We are fans of STRIDE and LINDDUN. However in the context of the TM sessions we organize other approaches are just fine.
- We organize regular threat modeling brainstorming sessions in person that are scheduled for about 2-3 hours.
- We always start the workshop by revisiting the application risk profile. The risk profile contains amongst others the list of assumptions, constraints and set of events our organization can and cannot tolerate.
- Then one of the software architects draws a data flow diagram on a dry-erase board. The team is free to jump in with additional details during this process.
- From this point on it's a freestyle brainstorming session where we start to look into

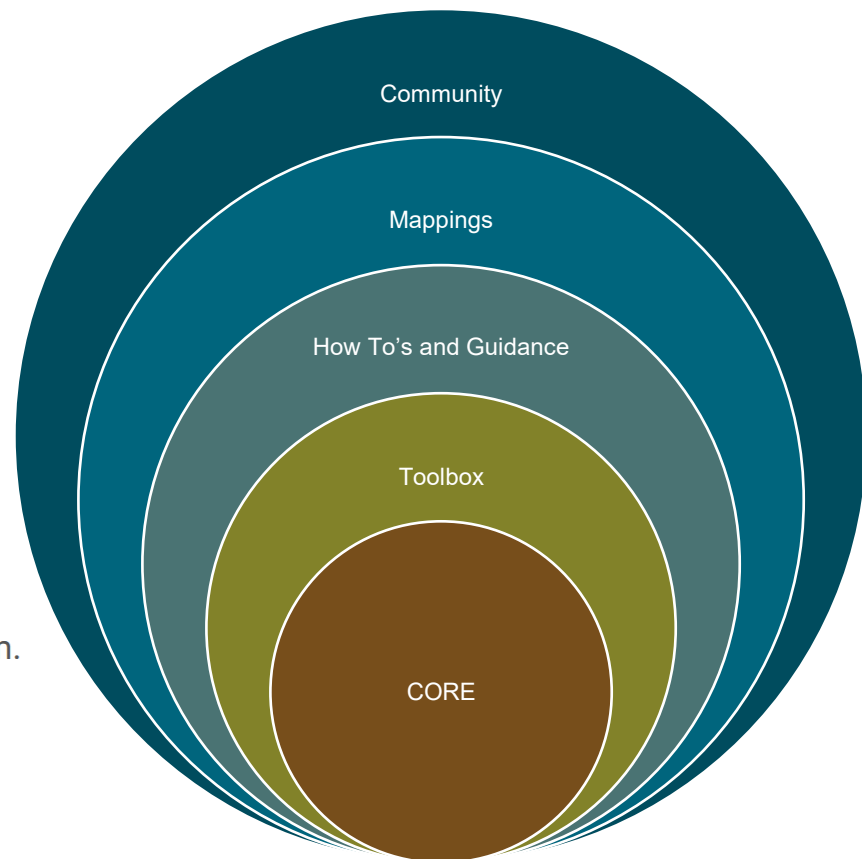
<https://owaspsamm.org/stream-guidance/>

Stream Guidance

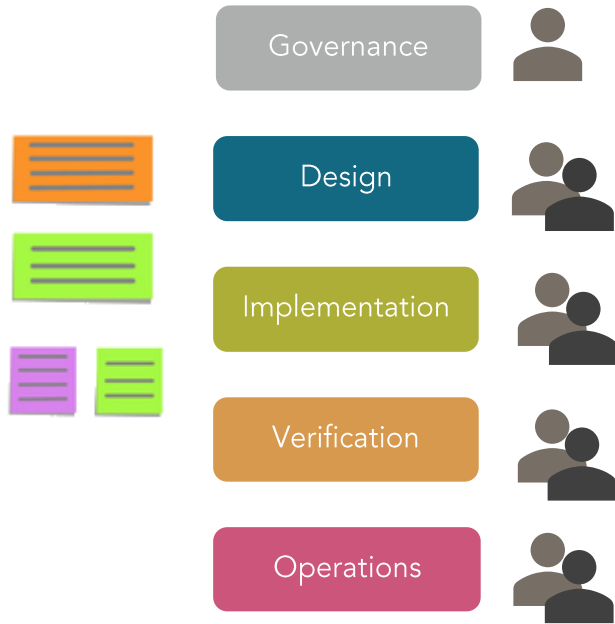
- **SAMM team** guidance [Google Doc](#) 
- **Community** guidance [Google Doc](#) 

Want to contribute?

Complete this [Google Form](#)  with guidance for this Stream.



THE TEAM OWNS THE ROADMAP

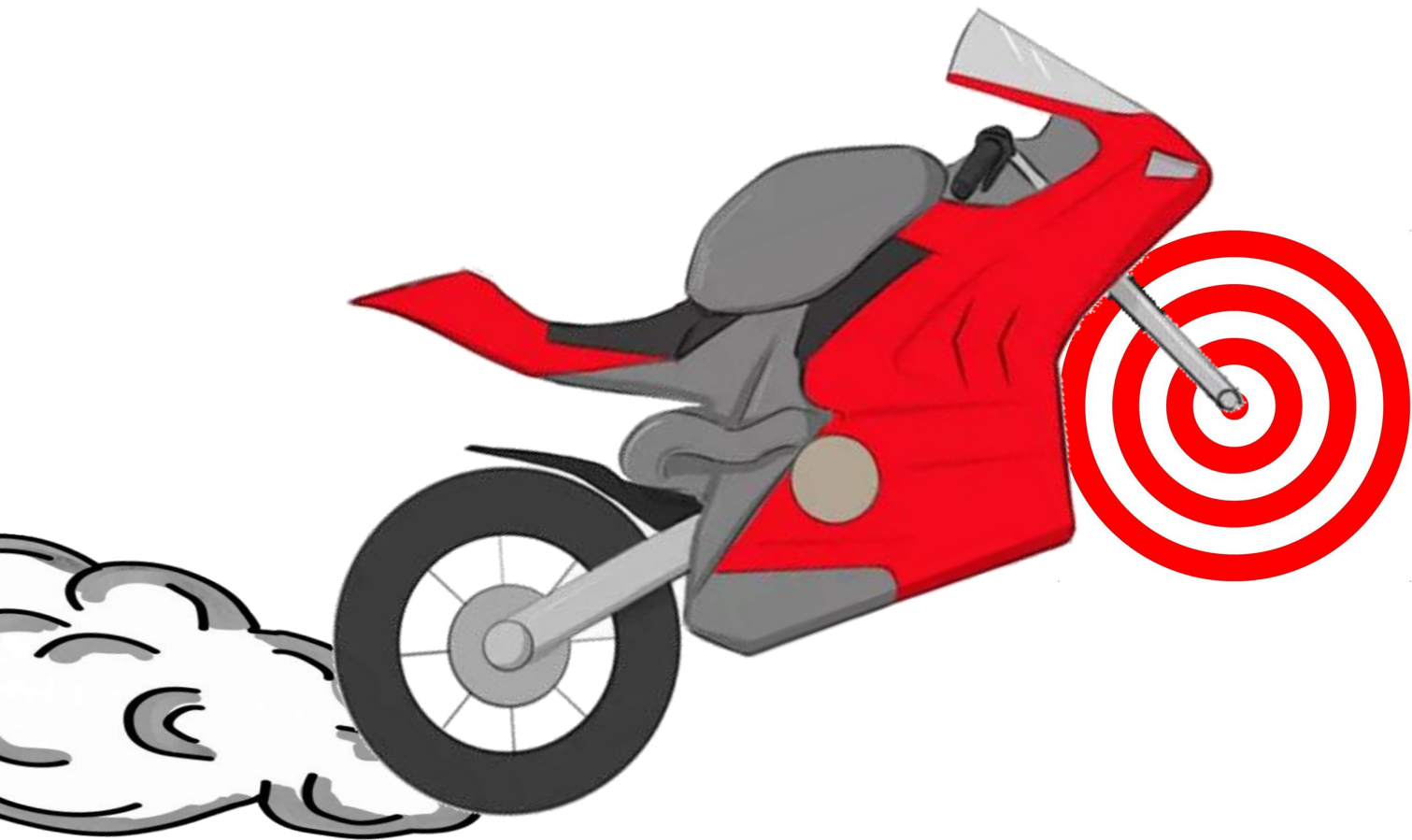


***"You get
what you measure"***

■ 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

$$\text{PercentToTarget} = 1 - \text{Gap} / \text{Target}$$

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

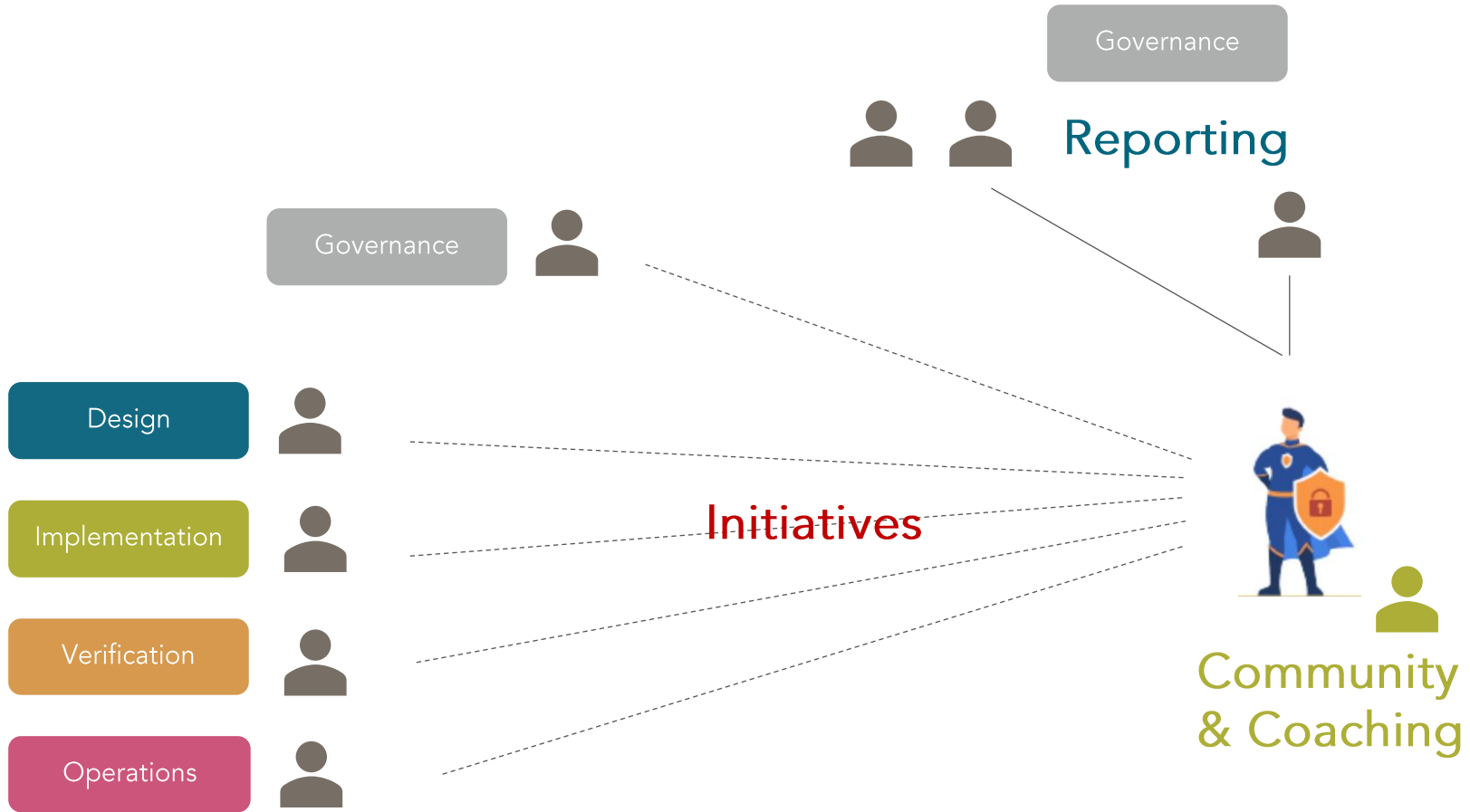
Need to improve

"Not applicable"

* Gap is zeroed out to avoid giving credit for "overshooting"

THE TEAM OWNS THE ROADMAP





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

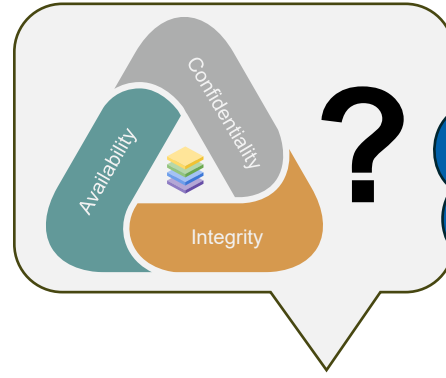
→ Use initiatives to support team progress



**SAMM:
12-24m**



**Roadmap
Progress:
3-6m**



Common context

Common language

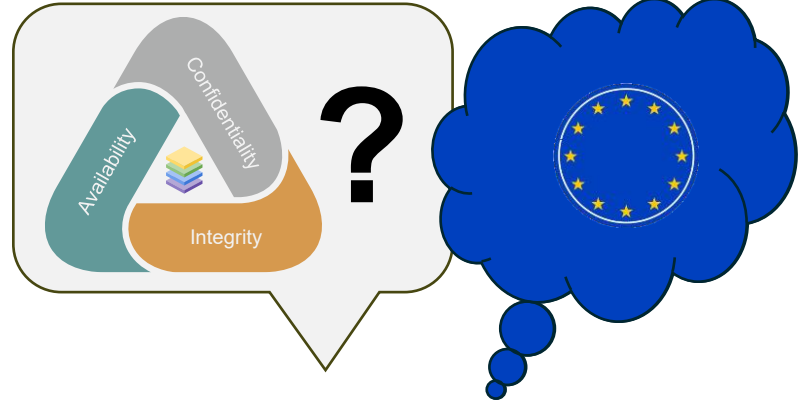
Clear delineation of shared responsibilities

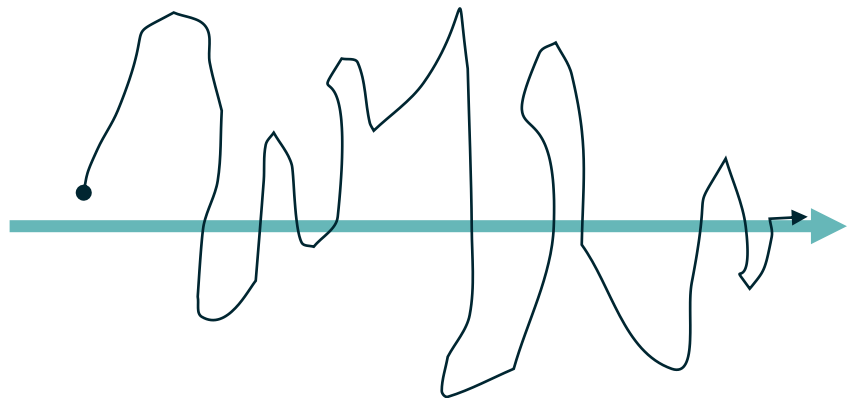


WHAT



HOW

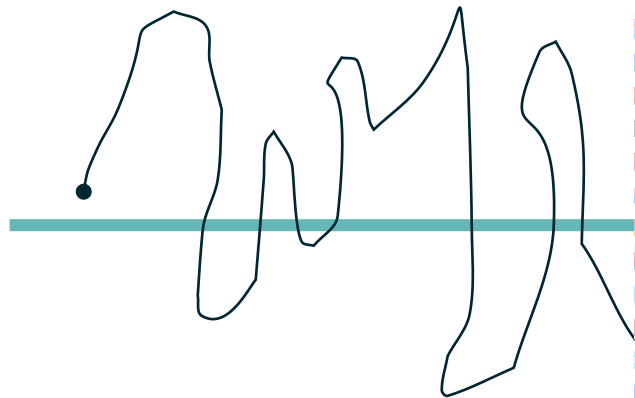




WHAT



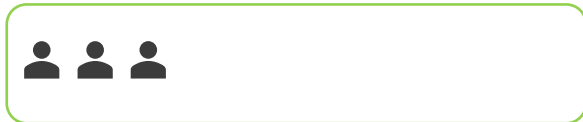
HOW



WHAT



HOW



Targets



Initiatives







owaspsamm.org



github.com/owaspsamm



[#project-samm](https://twitter.com/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

