secure habits

xygeni.

OWASP Stuttgart

EU CRA in Practice

SAMM as a Compliance Foundation

Nariman Aga-Tagiyev

February 17th 2026

Agenda

1. Introduction to CRA
2. A High-Level look at SAMM
3. Deep dive into the SAMM
4. Industry Benchmarks
5. Soft and hard challenges
6. Next steps

Introduction

Build secure habits in software development teams

Nariman Aga-Tagiyev

- Founder of SecureHabits
- Application Security Architect
- OWASP SAMM core team member
- ISO 27034 WG OWASP liaison
- Secure coding and threat modeling trainer
- 24 years in software development, 9 years in product security
- Xygeni Implementation Partner

xygeni. secure habits

CRA

Why

- ❏ Force some level of product security
- ❏ Have better informed consumers

When

- ❏ End of 2026 for the notification obligations
- ❏ End of 2027 for the full applicability

Who has to comply?

- ❏ All products with digital elements

CRA - an EU Regulation

FEATURE	EU Regulation	EU Directive
Directly Applicable?	✔ Yes	✘ No
Needs national legislation?	✘ No	✔ Yes
Uniform across EU?	✔ Fully	✘ Varies
Binding?	✔ Entirely	✔ In terms of goals only
Flexible for countries	✘ None	✔ Yes

GDPR CRA NIS2

NIS2

Directive

Protects the critical sectors, the organizations operating in them, and everyone who depends on their continuity and security.

CRA

Regulation

Aims to protect consumers and businesses by ensuring that all products are secure throughout their entire lifecycle

European Regulation

Cybersecurity requirements as part of the CE marking

for ‘Products with Digital Elements‘

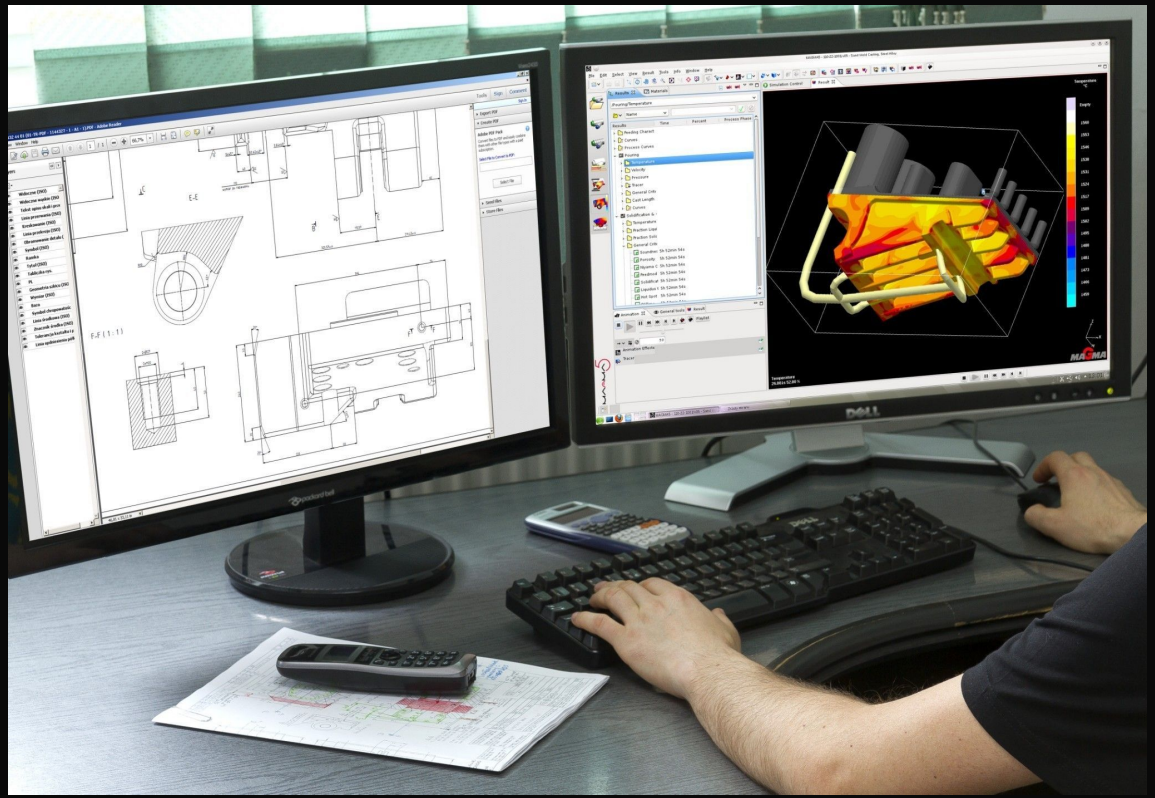
Published in the Official Journal Of The European Union on 20/11/2024

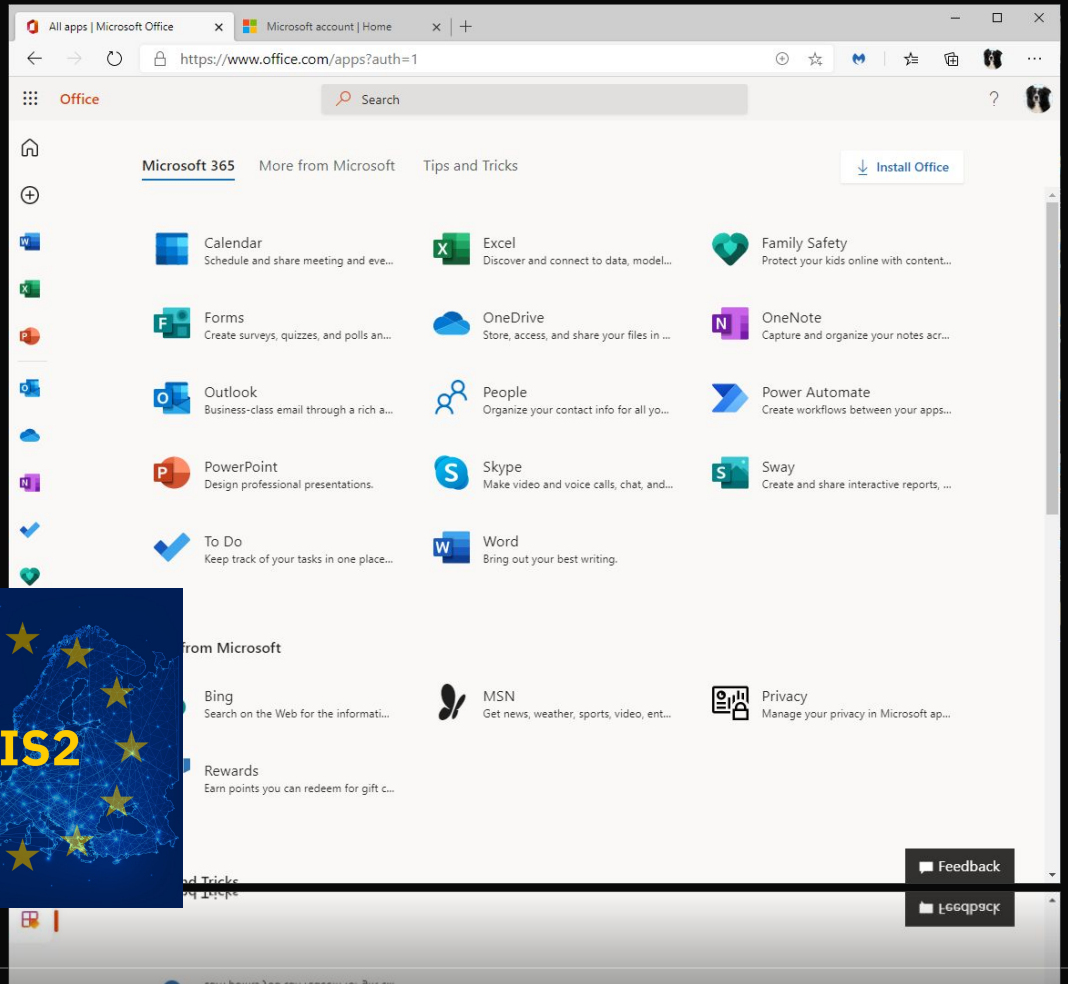
Products with Digital Elements

A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately


ELECTRANGES
16.19
05:95
£0.59
KITCHER
emo
Notal Canter
Betchonies

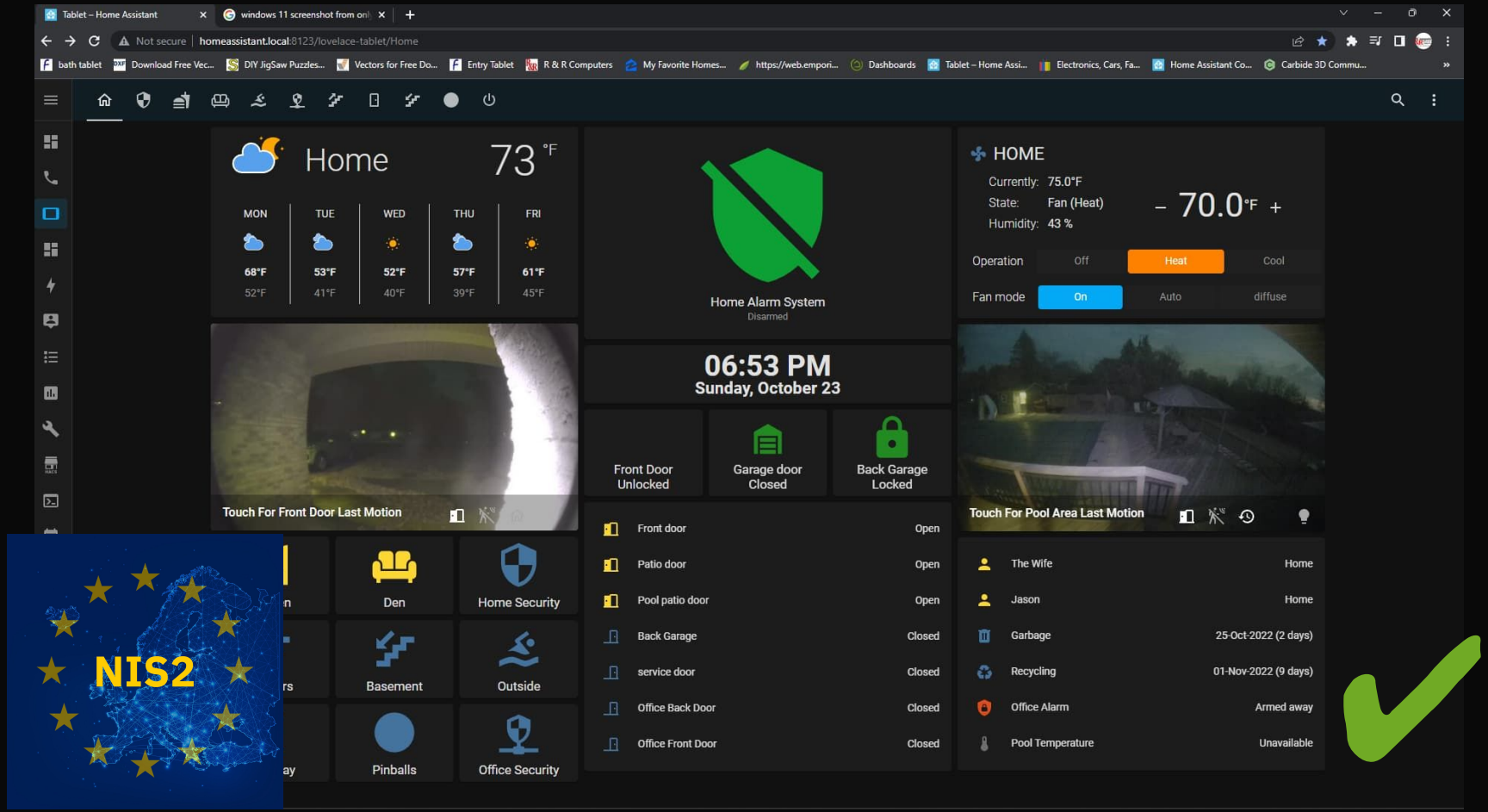

Windows Vista
Home Premium
159




All apps | Microsoft Office
Microsoft account | Home
https://www.office.com/apps?auth=1
Office
Search
Microsoft 365
More from Microsoft
Tips and Tricks
Install Office
Calendar
Schedule and share meeting and eve...
Excel
Discover and connect to data, model...
Family Safety
Protect your kids online with content...
Forms
Create surveys, quizzes, and polls an...
OneDrive
Store, access, and share your files in ...
OneNote
Capture and organize your notes acr...
Outlook
Business-class email through a rich a...
People
Organize your contact info for all yo...
Power Automate
Create workflows between your apps...
PowerPoint
Design professional presentations.
Skype
Make video and voice calls, chat, and...
Sway
Create and share interactive reports, ...
To Do
Keep track of your tasks in one place...
Word
Bring out your best writing.
rom Microsoft
Bing
Search on the Web for the informati...
MSN
Get news, weather, sports, video, ent...
Privacy
Manage your privacy in Microsoft ap...
Rewards
Earn points you can redeem for gift c...
Feedback

NIS2

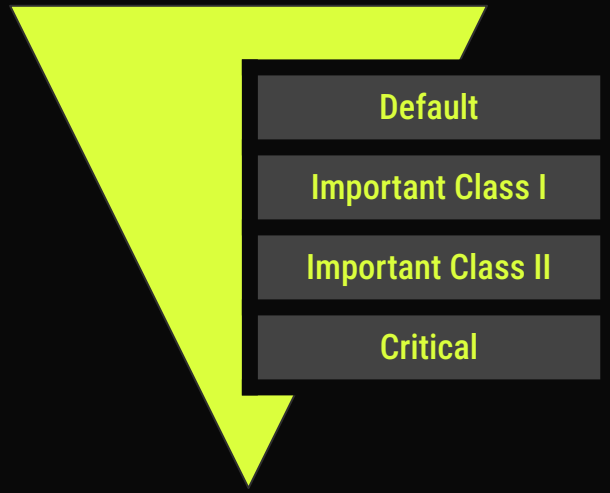

Microsoft
Edge
Excel
Office
OneNote
Microsoft Stream
Outlook
PowerPoint
Teams


Tablet – Home Assistant
windows 11 screenshot from onl
Not secure
homeassistant.local:8123/lovelace-tablet/Home
Home
73 °F
MON
TUE
WED
THU
FRI
68°F
52°F
53°F
41°F
52°F
40°F
57°F
39°F
61°F
45°F
Home Alarm System
Disarmed
HOME
Currently: 75.0°F
State: Fan (Heat)
Humidity: 43 %
70.0°F
Operation
Off
Heat
Cool
Fan mode
On
Auto
diffuse
06:53 PM
Sunday, October 23
Front Door Unlocked
Garage door Closed
Back Garage Locked
Touch For Front Door Last Motion
Touch For Pool Area Last Motion
Den
Home Security
Basement
Outside
Pinballs
Office Security
Front door Open
Patio door Open
Pool patio door Open
Back Garage Closed
service door Closed
Office Back Door Closed
Office Front Door Closed
The Wife Home
Jason Home
Garbage 25-Oct-2022 (2 days)
Recycling 01-Nov-2022 (9 days)
Office Alarm Armed away
Pool Temperature Unavailable
NIS2

Pepperoni pizza machine

CRA

Product Classification



Default

Lowest Risk Category

Examples

- General-purpose software and apps
- Standard office IT hardware
- Smart office / IoT devices
- Consumer-like devices used in business

Assessment

- Manufacturers can perform a self-assessment (Module A).
- The manufacturer retains the flexibility to choose a stricter conformity assessment procedure involving a third party if they wish (CRA Art. 32 § 1, CRA Rec. 93)

Class I

Elevated Cybersecurity Risk

Examples

- ❏ Password managers
- ❏ Standalone and embedded browsers
- ❏ SIEM systems
- ❏ Identity management systems software

Assessment

- ❏ Self-assessment (Module A) is possible if the manufacturer fully applies relevant harmonised standards.
- ❏ Otherwise, a third-party audit is required (CRA Art. 32 § 2).

Class II

Significant Risk of Disruption

Examples

- ❏ OS for servers, desktops, mobile devices
- ❏ Firewalls and intrusion detection or prevention systems
- ❏ Industrial intrusion detection systems
- ❏ Tamper-resistant microprocessors

Assessment

- ❏ A third-party audit by a Notified Body is mandatory (CRA Art. 32 § 3)

Critica
l

EU Critical Infrastructure

Examples

- Smart meter gateways
- Hardware Security Modules (HSMs)
- Smart cards and secure elements

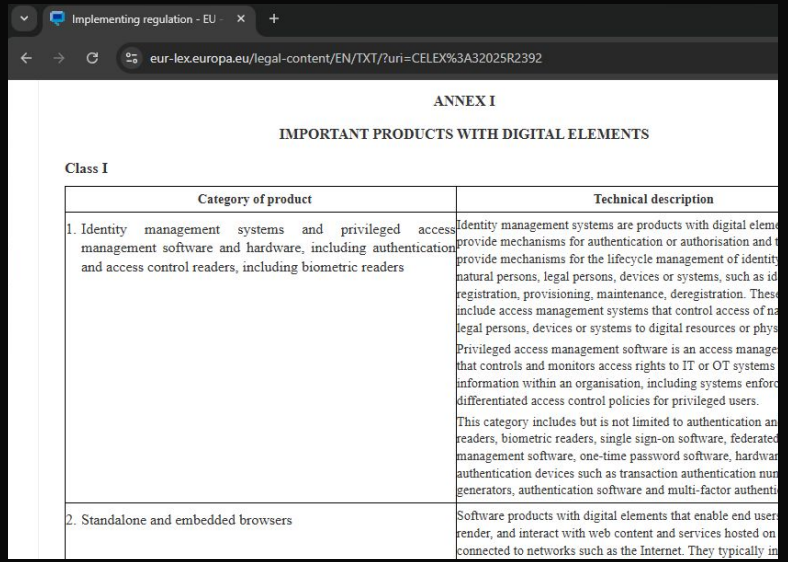
Assessment

- The Commission may require a mandatory European cybersecurity certificate (external audit) at assurance level 'substantial' or higher.
- If no such scheme is mandated, these products follow the same rules as Class II (CRA Art. 32 § 4).

Formal resource with product examples

EUR-Lex Access to European Union law website has detailed examples of products for each category.

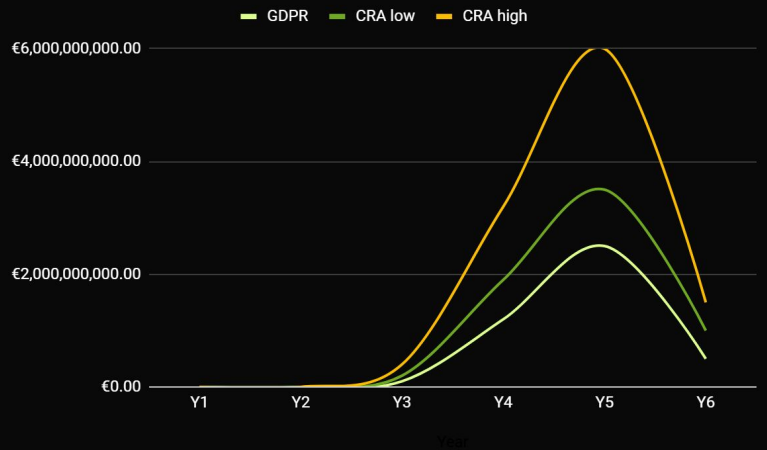
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R2392



Expected fines

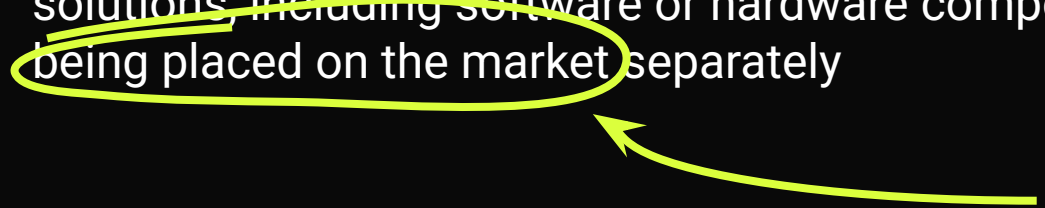
Non-Compliance

- **Up to €15M or 2.5% of the yearly global turnover** for nonconformity with essential requirements
- **Up to €10M or 2% of the yearly global turnover** for failing to meet administrative requirements
- **Up to €5M or 1% of the yearly global turnover** for misleading market surveillance authorities
- Loss of the CE - no EU market access



Products with Digital Elements

A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately

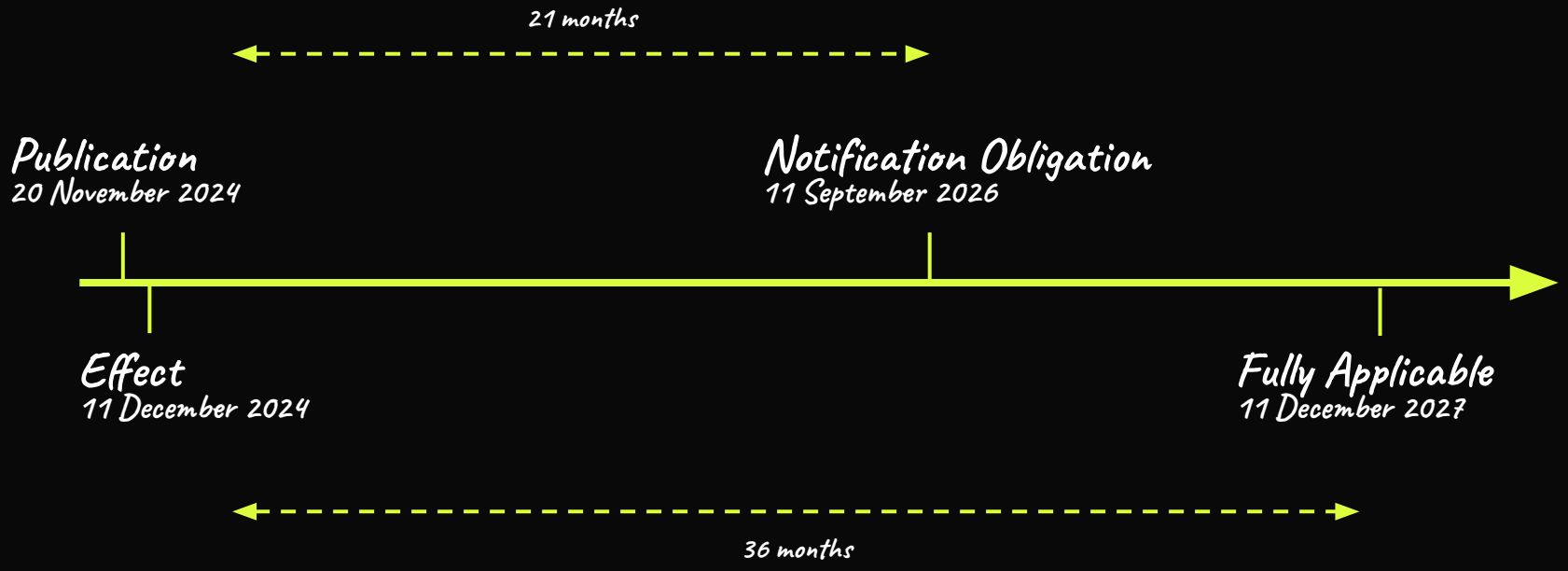


“Being placed”

Products are “placed on the market” by a manufacturer or an importer when they supply a product to a distributor or 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

Fully Applicable
11 December 2027


21 months
Publication
20 November 2024
Notification Obligation
11 September 2026
Effect
11 December 2024
Fully Applicable
11 December 2027
36 months

- ✓ Manufacturers are obligated to report actively exploited vulnerabilities and security incidents to National CERT and ENISA (European Union Agency for Cybersecurity) within 24 hours of becoming aware, with a follow-up report required within 72 hours and a final report within 30 days.

- ✓ They must also inform users of the incident and provide guidance or mitigation steps.

For all the products that have ever been put on the market!

Publication
20 November 2024

Effect
11 December 2024

Notification Obligation
11 September 2026

Fully Applicable
11 December 2027

- ✓ Declaration of Conformity
- ✓ Technical documentation
- ✓ Secure by Design & Secure by Default
- ✓ Vulnerability Management
- ✓ Risk-based security requirements !!

Shared Responsibility

- There will be no checklist for compliance!
- Every manufacturer needs to define own reasonable requirements and controls based on Risk Analysis
- Standards are being developed as a guidance for this process

5 years SSDLC support after release

Supporting standards are on the way

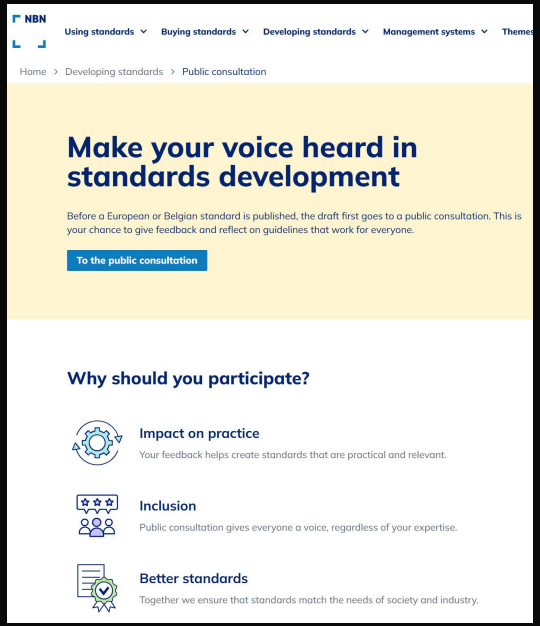
- 30/08/2026: Principles of Cyber Resilience
- 30/08/2026: Vulnerability Management
- 30/10/2027: Security Requirements
- 30/10/2026: Important and critical products

Public enquiry

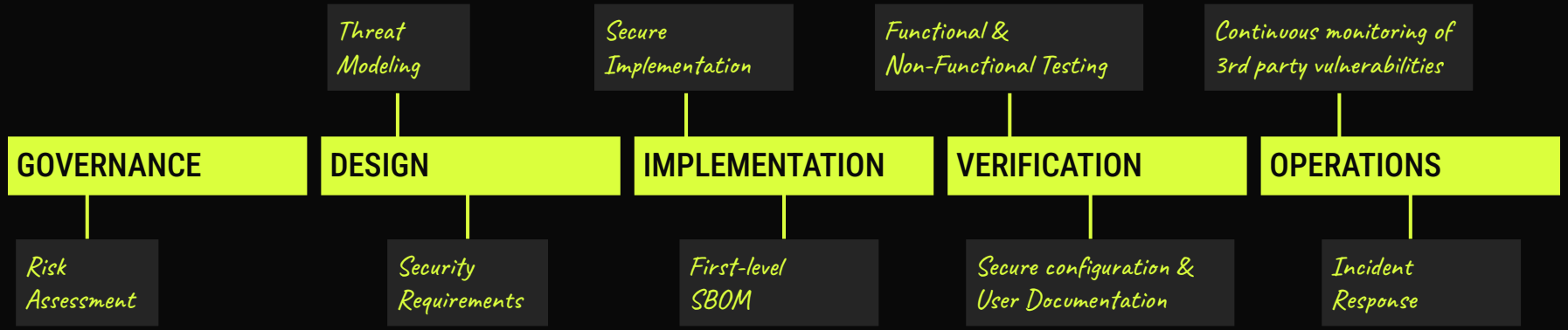
- You can read and contribute to the early standard drafts on public enquiry pages.

- European Draft Standards references:
  prEN-40000-1-1:2025
  prEN-40000-1-2:2025

https://www.nbn.be/en/standards-development/public-enquiry
https://www.stan4cra.eu/etsi-tc-cyber

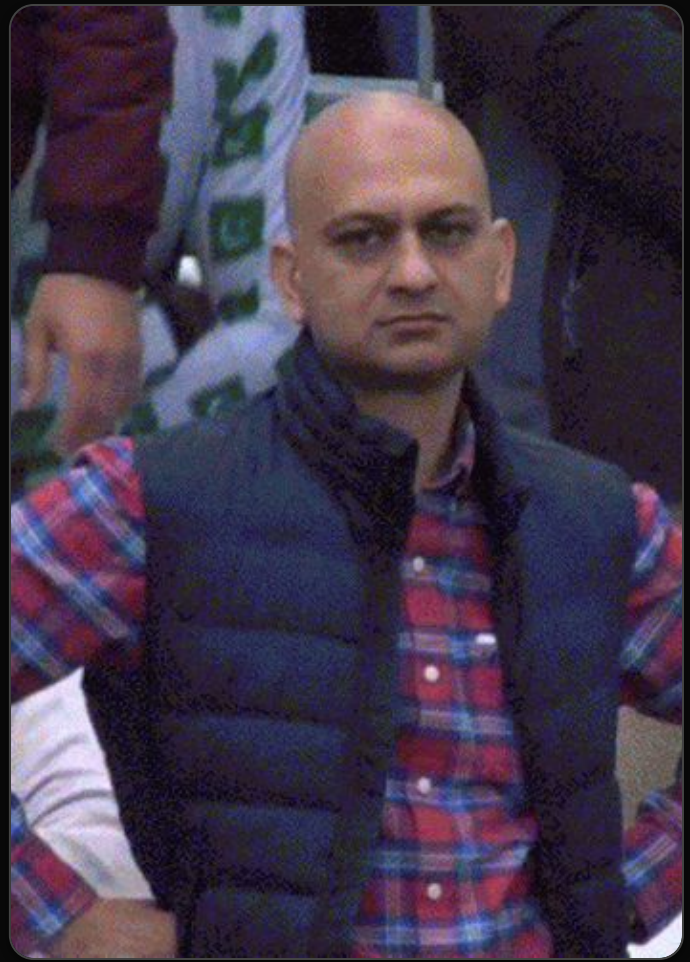


Secure SDLC


Threat Modeling
Secure Implementation
Functional & Non-Functional Testing
Continuous monitoring of 3rd party vulnerabilities
GOVERNANCE
DESIGN
IMPLEMENTATION
VERIFICATION
OPERATIONS
Risk Assessment
Security Requirements
First-level SBOM
Secure configuration & User Documentation
Incident Response

Get Ready!

Let your Legal department take care of it?



Maturity Frameworks

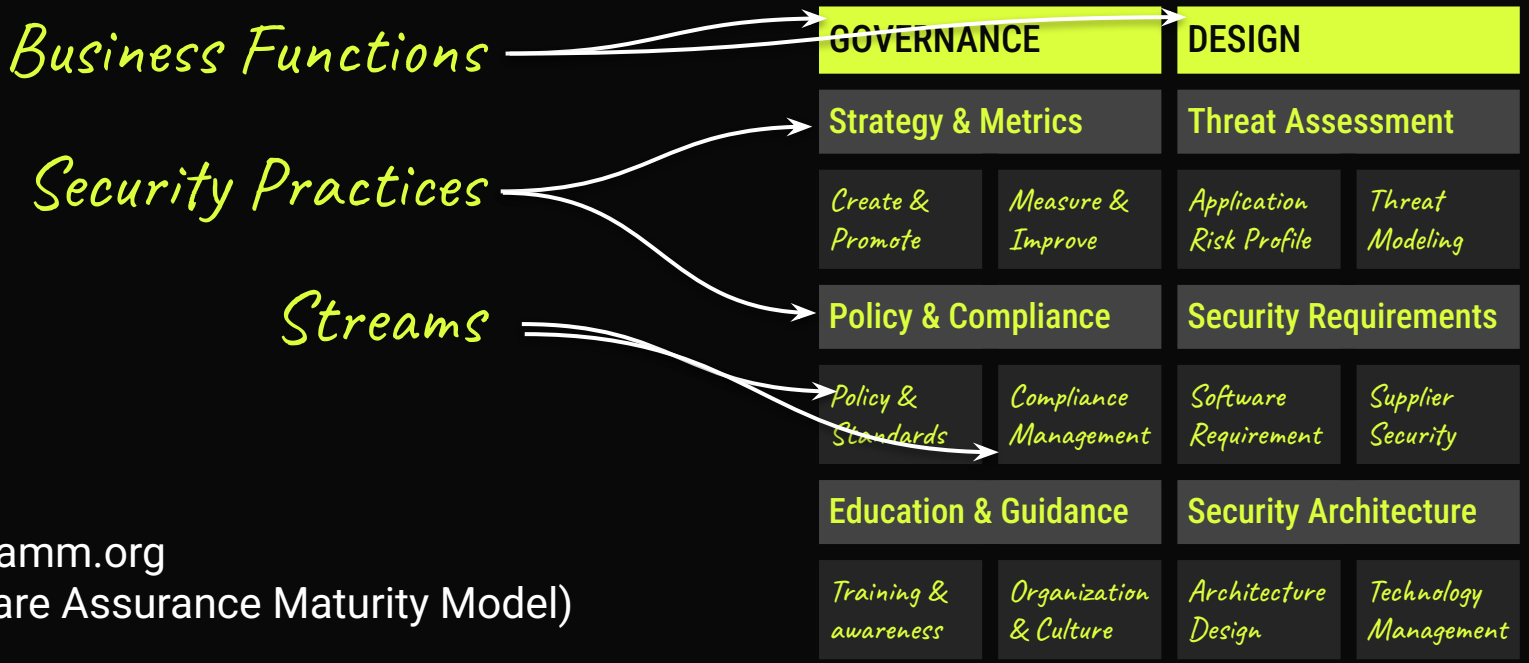
Structured frameworks to evaluate and enhance security across business functions. These frameworks also aid in documenting the Software Security Development Lifecycle (SSDL) in a structured way.

BSIMM

The SAMM 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 SAMM Model



https://owaspsamm.org
(OWASP Software Assurance Maturity Model)

Activity Level 1 / 2 / 3

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 …

Maturity Level 1 / 2 / 3

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 / 2 / 3

Answers

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

Stream Guidance

SAMM team guidance Google Doc 🔗
Community guidance Google Doc 🔗

Assess

One scope at a time

Set target

Tailored for a scope

Work the plan

Tip: Use SAMM Community Guidance

Set target

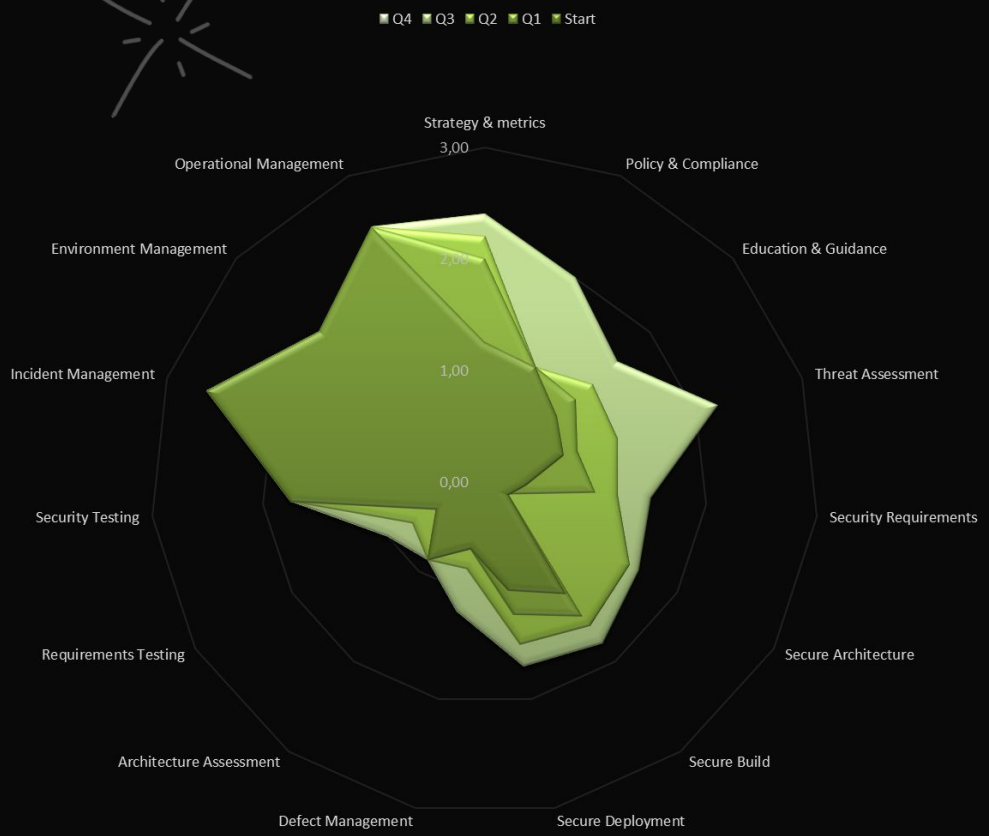
Tailored for a scope

Work the plan

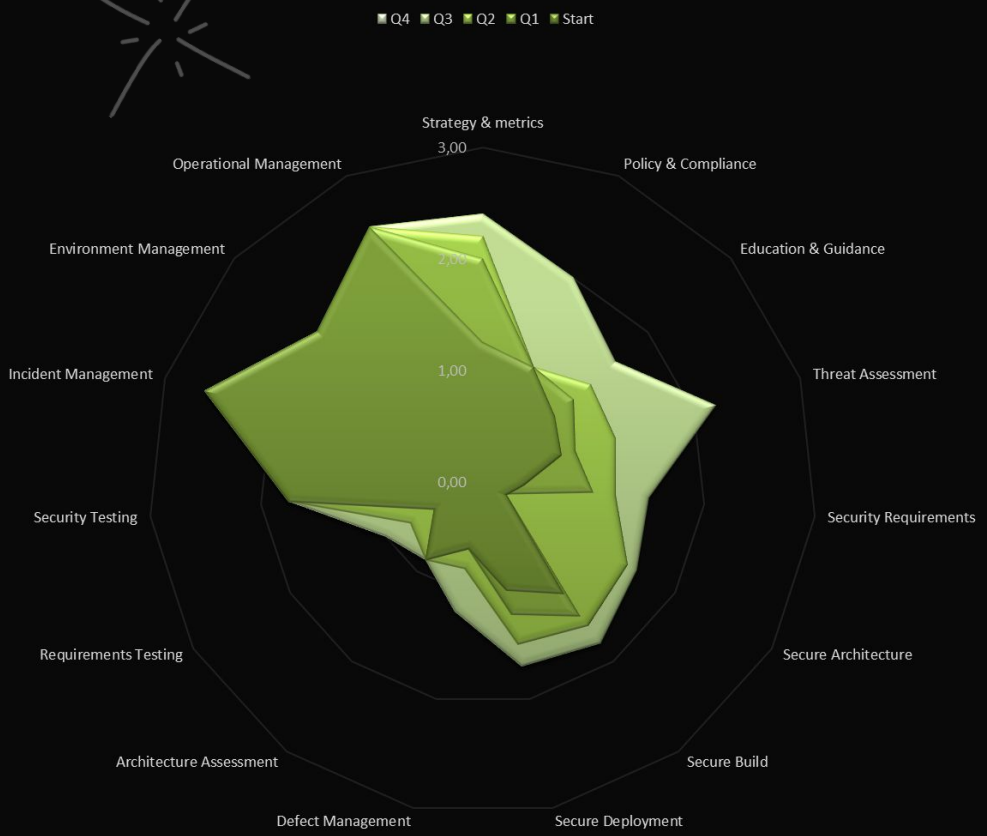
Tip: Use SAMM Community Guidance

Set target

Tailored for a scope



Work the plan



Tip: Use SAMM Community Guidance

But how to set a target?

1. Product & Architecture Discovery

System of Interest definition:

Define scope: what part of the system we are going to focus

Stakeholder interest definition:

Why the system is needed and what are the main objectives of the end user

- Document
  - Architecture Diagrams
  - Trust Boundaries
  - Data Flow Diagrams
  - Infrastructure and dependencies
  - Deployment, update

2. Product Risk Assessment

Perform Threat Modeling, focusing on threats relevant to the end-user.

Identify unacceptable risks for the product user.

- Assess Impact:
  - Safety
  - Availability
  - Confidentiality
  - Internal, external, third-party harms

3. Derive Security Requirements

Goal: Translate risks to security requirements

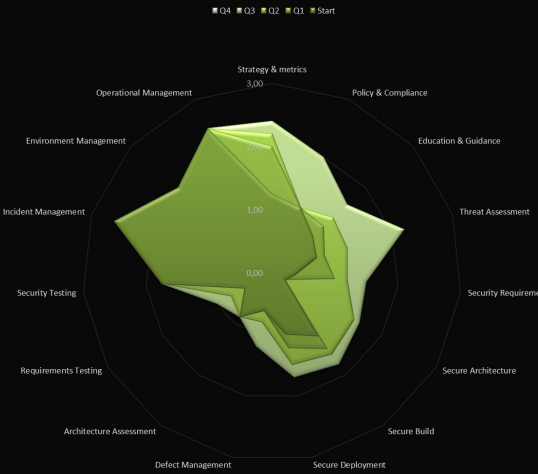
Define secure-by-design and secure-by-default expectations

SAMM Activities CRA risk criticality

- Deliverables
  - Product Security Requirements document
  - CRA Annex I mapping (essential security requirements)

4. OWASP SAMM Baseline Assessment

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*



4. Prioritize AppSec Activities

Goal: Avoid “let’s do everything” paralysis.

Priority => CRA Risk Criticality
× SAMM Maturity Gap

Fulfill dev-related dutiesæ

CRA flow summary

1. Architecture discovery
2. CRA risk assessment (product-focused)
3. Security requirements derivation
4. SAMM baseline assessment
5. Risk × maturity prioritization
6. Target SAMM definition
7. Implementation roadmap
8. Evidence & lifecycle ops

SAMM Benchmark

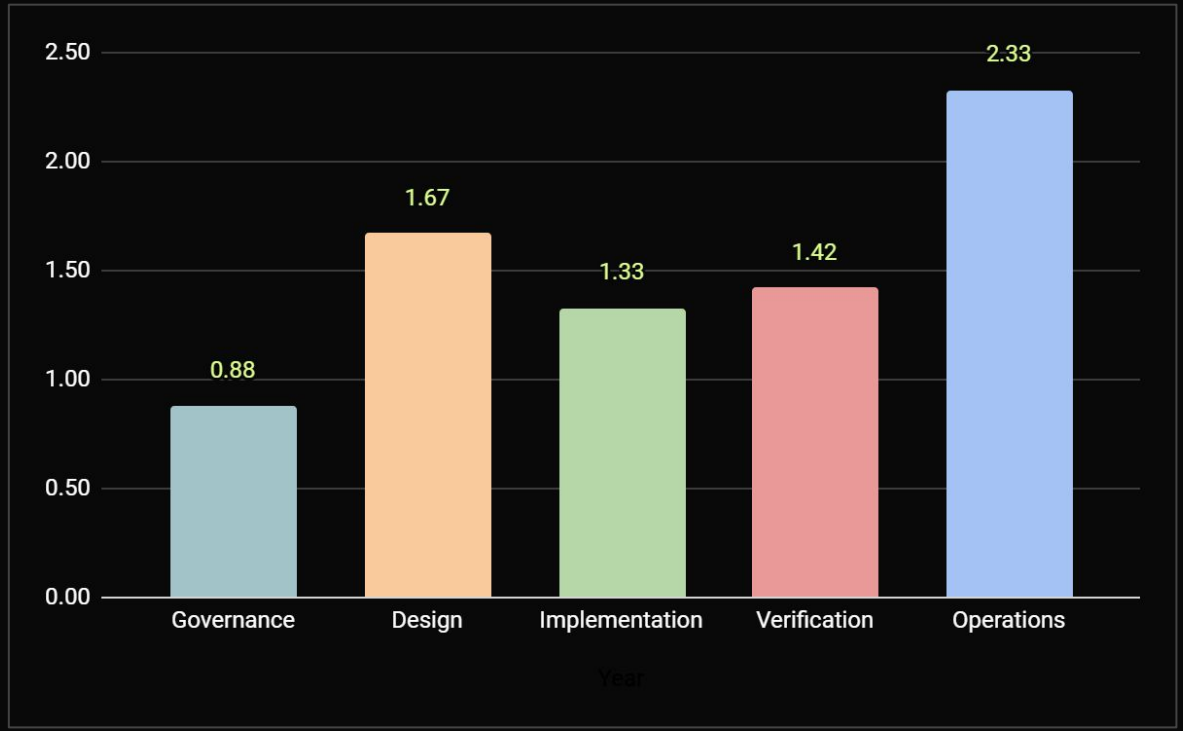
How do I compare to similar organizations?

https://owaspsamm.org/benchmark/

SAMM to CRA mapping

CRA Low Baseline

Minimum SAMM posture

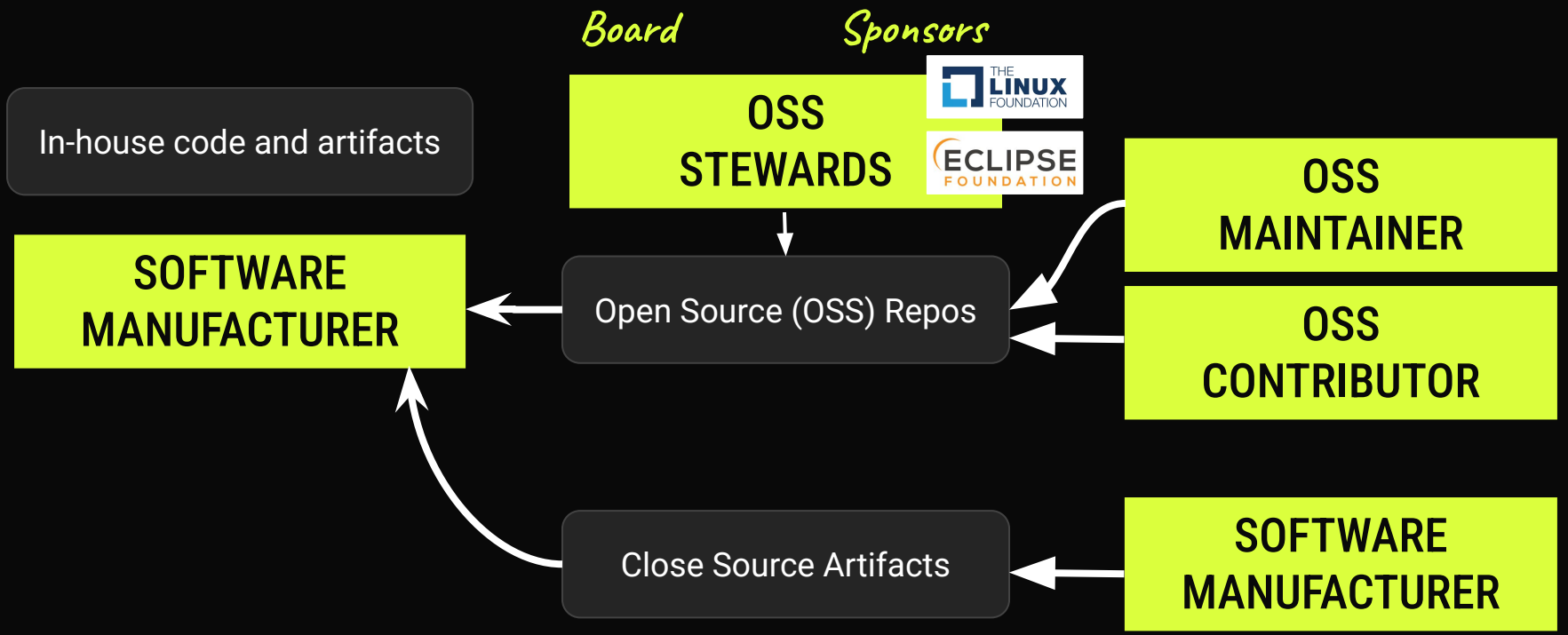


Top Gaps

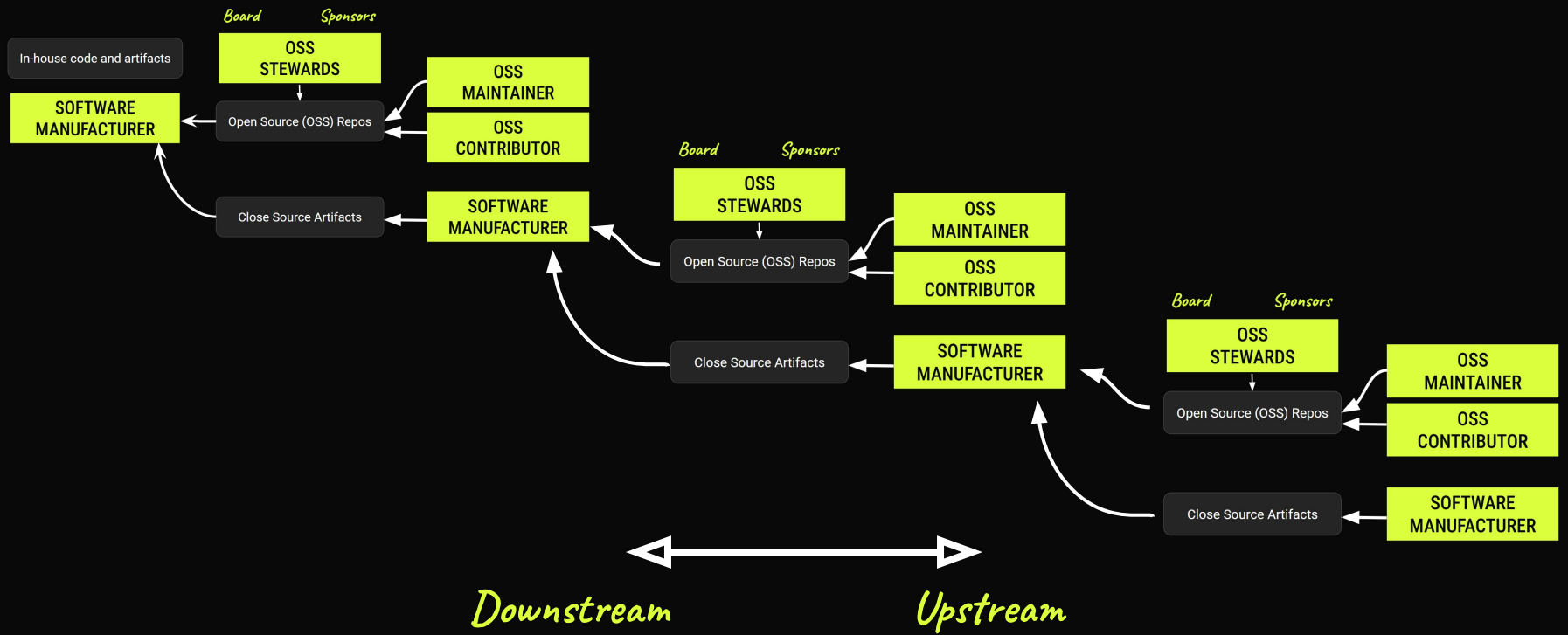
OWASP SAMM ACTIVITY	CRA NEEDS	INDUSTRY TODAY (SAMM Benchmark)	GAP
Threat Assessment: Application Risk Profile	3	1.42	-1.58
Threat Assessment: Threat Modeling	2	0.82	-1.18
Environment Management: Patch and Update	3	1.86	-1.14
Defect Management: Defect Tracking	3	1.87	-1.13
Operational Management: Legacy Management	3	1.87	-1.13
Architecture Assessment: Architecture Mitigation	2	0.9	-1.1

New era for the Software Supply Chain

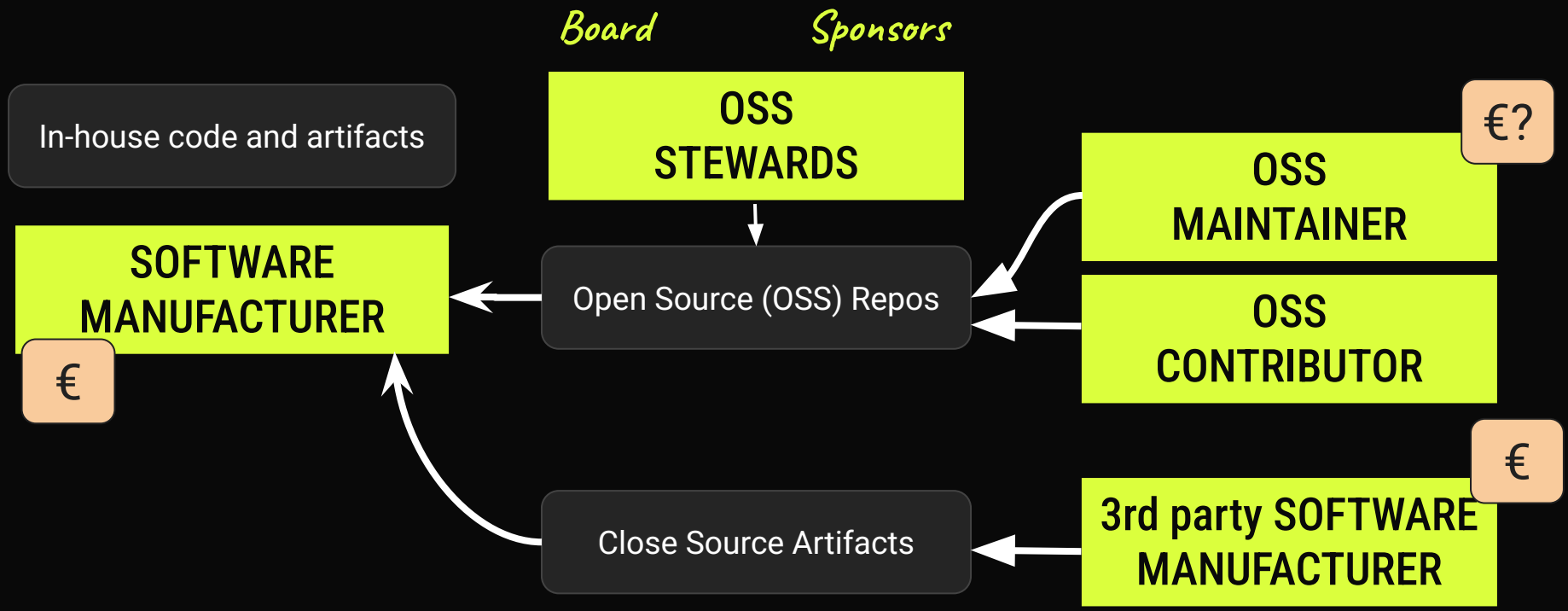
OSS Stakeholders



OSS Supply Chain



CRA Liability



Fulfill dev-related dutiesæ

Obligations for Manufacturers

1. Ensure security by design
2. Maintain documentation
3. Evidence availability
4. Notification obligation (CSIRT, ENISA, Users)

Fulfill dev-related dutiesæ

Obligations for the OSS Stewards

1. Adopt cybersecurity policy
2. Cooperate with authorities
3. Fulfill dev-related duties

Fulfill dev-related dutiesæ

Obligations for the OSS Maintainers

If commercialized:

1. Ensure security by design
2. Handle vulnerabilities
3. Maintain tech. documentation

Fulfill dev-related dutiesæ

Obligations for the OSS Contributors

- No obligations if:
  - Not monetizing commercially
- Act as manufacturer if:
  - Monetizing (paid support, bundle with commercial services)

Can SAMM help you with CRA?

You are here

1. ~~Introduction to CRA~~
2. ~~A High Level look at SAMM~~
3. Deep dive into the SAMM
4. Industry Benchmarks
5. Soft and hard challenges
6. Next steps

Take Aways

CRA affects your market access

- ❏ EU CRA can be used to control the EU market
- ❏ Continuous documentation and evidence required

Use OWASP SAMM

- ❏ Community guidelines available for you
- ❏ It’s about a journey to become more mature

CRA requirements -> risk based

- ❏ Legal department cannot come up with a checklist
- ❏ This time it’s a true teamwork between legal and dev

secure habits

Thank you!

Questions & Answers

/aganariman

securehabits.nl

EU CRA Health check

Nariman Aga-Tagiyev

1 hr

A one-hour CRA health check to identify gaps in the company's current CRA readiness strategy.