

From Maturity to Mastery: Accelerating Software Security with OWASP SAMM



Software Assurance Maturity Model



Measurable

Defined maturity levels across business practices



Actionable

Clear pathways for improving maturity levels



Versatile

Technology, process, and organization agnostic

Governance

Strategy and Metrics

Create and
promote

Measure and
improve

Stream A

Stream B

Policy and Compliance

Policy &
standards

Compliance
management

Stream A

Stream B

Education and Guidance

Training and
awareness

Organization
and culture

Stream A

Stream B

Design

Threat Assessment

Application
risk profile

Threat
modeling

Stream A

Stream B

Security Requirements

Software
requirements

Supplier
security

Stream A

Stream B

Secure Architecture

Architecture
design

Technology
management

Stream A

Stream B

Implementation

Secure Build

Build
process

Software
dependencies

Stream A

Stream B

Secure Deployment

Deployment
process

Secret
management

Stream A

Stream B

Defect Management

Defect
tracking

Metrics and
feedback

Stream A

Stream B

Verification

Architecture Assessment

Architecture
validation

Architecture
mitigation

Stream A

Stream B

Requirements-driven Testing

Control
verification

Misuse/abuse
testing

Stream A

Stream B

Security Testing

Scalable
baseline

Deep
understanding

Stream A

Stream B

Operations

Incident Management

Incident
detection

Incident
response

Stream A

Stream B

Environment Management

Configuration
hardening

Patch and
update

Stream A

Stream B

Operational Management

Data
protection

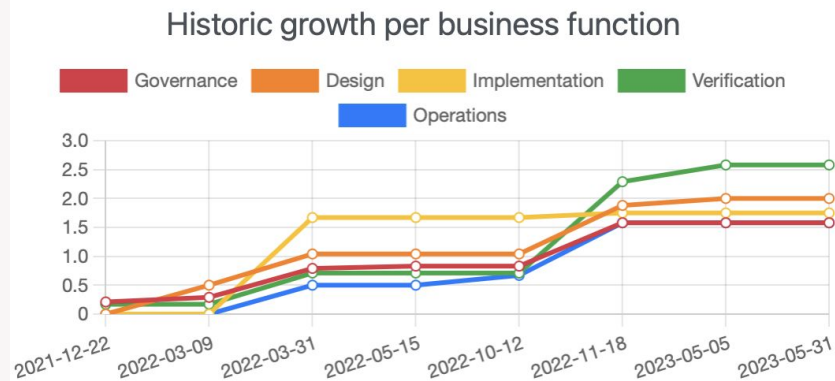
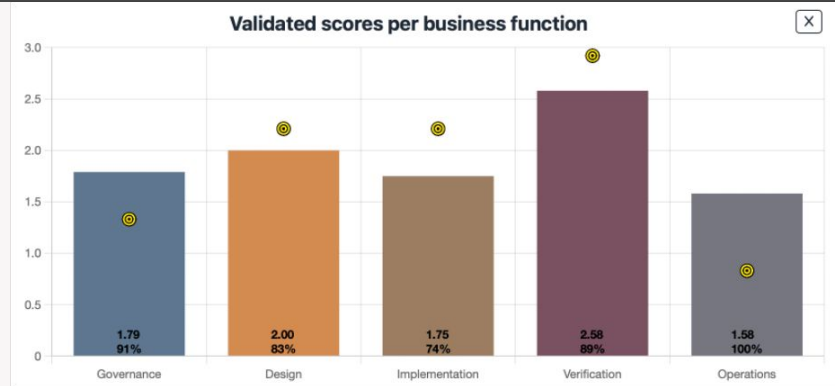
Legacy
management

Stream A

Stream B

Scorecards

- Evaluate existing practices
- Gap analysis
- Build a balanced improvement program
- Demonstrate improvements
- M&A assessments
- Negotiate cheaper cybersecurity premiums



SAMM Stream (Software Dependencies)

Maturity level	Software Dependencies
Level 1: Ad-hoc provisioning	Create records with Bill of Materials of your applications and opportunistically analyze these.
Level 2: Effectiveness and efficiency	Evaluate used dependencies and ensure timely reaction to situations posing risk to your applications.
Level 3: Comprehensive mastery	Analyze used dependencies for security issues in a comparable way to your own code.

Do you have solid knowledge about dependencies you're relying on?

Answers

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

Quality criteria

- You have a current bill of materials for every application
- You can quickly find out which applications are affected by a particular CVE
- You have analyzed, addressed, and documented findings from dependencies at least once in the last three months

Self-paced OWASP SAMM training

OWASP SAMM

Fundamentals Course

About this course

-  Free
-  79 lessons
-  5 hours of video content



owaspsamm.thinkific.com/courses/samm

Sponsored by



Assessment tools



Spreadsheets

Google Sheets (Google Drive)

Excel (GitHub)

SAMMwise

Open source, self-hosted solution

<https://github.com/owaspsamm/sammwise>

Open SAMMY

Open source, self-hosted solution

<https://github.com/OWASP/open-sammy>

SAMM Assessment Guidance

Guidelines and best practices

owaspsamm.org/assessment

Example questions

[SAMM assessment Drive folder](#)

Podcast

[SAMM Podcast - Assessment on our YouTube channel](#)



Mappings to/from other frameworks

- NIST SSDF, NIST CSF 2.0, IEC 62443-4-1, BSIMM 14
- Threat Modeling Capabilities
- Microsoft SDL
- OWASP DSOMM
 - <https://dsomm.owasp.org/mapping>



OpenCRE mapping

 OpenCRE

HomeBrowseOpenCRE ChatMap Analysis

Search...  Search

Describe high-level system architecture and perform threat modeling on it every critical change and regularly

CRE: 068-102

Which is linked to sources:

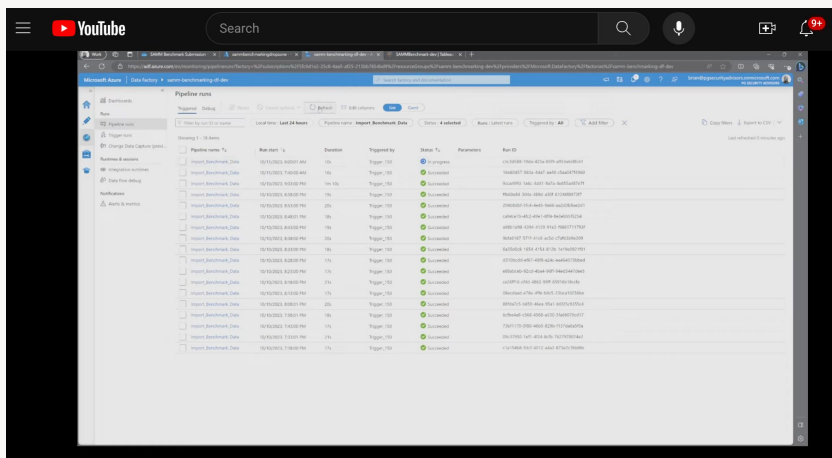
- Standard : ASVS : V1.1.5 : Verify definition and security analysis of the application's high-level architecture and all connected remote services. [↗](#)
- Standard : CWE : 1059 [↗](#)
- Standard : DevSecOps Maturity Model (DSOMM) : 0a929c3e-ab9a-4206-8761-adf84b74622e : Design : Creation of advanced abuse stories [↗](#)
- Standard : DevSecOps Maturity Model (DSOMM) : 47419324-e263-415b-815d-e7161b6b905e : Design : Conduction of simple threat modeling on technical level [↗](#)
- Standard : DevSecOps Maturity Model (DSOMM) : 48f97f31-931c-46eb-9b3e-e2fec0cd0426 : Design : Conduction of simple threat modeling on business level [↗](#)
- Standard : DevSecOps Maturity Model (DSOMM) : ae22dafd-bcd6-41ee-ba01-8b7fe6fc1ad9 : Design : Conduction of advanced threat modeling [↗](#)
- Standard : DevSecOps Maturity Model (DSOMM) : bacf85b6-5bc0-405d-b5ba-a5d971467cc1 : Design : Creation of simple abuse stories [↗](#)
- Standard : DevSecOps Maturity Model (DSOMM) : dd5ed7c1-bdbf-400f-b75f-6d3953a1a04e : Design : Creation of threat modeling processes and standards [↗](#)
- Standard : DevSecOps Maturity Model (DSOMM) : f88d1b17-3d7d-4c3d-8139-ad44fc4942d4 : Education and Guidance : Regular security training of security champions [↗](#)
- Standard : NIST 800-53 v5 : SC-31 Covert Channel Analysis [↗](#)
- Standard : NIST SSDF : PW.1.1 : Use forms of risk modeling – such as threat modeling, attack modeling, or attack surface mapping – to help assess the security risk for the software.
- Standard : OWASP Cheat Sheets : Abuse Case Cheat Sheet [↗](#)
- Standard : OWASP Cheat Sheets : Attack Surface Analysis Cheat Sheet [↗](#)
- Standard : OWASP Cheat Sheets : Threat Modeling Cheat Sheet [↗](#)
- Standard : OWASP Proactive Controls : C1 [↗](#)
- Standard : SAMM : D-TA-B : Threat modeling [↗](#)

SAMM Benchmarking

How do I compare?

What works for similar organizations?

Donate
SAMM
data sets



The screenshot shows the SAMM Benchmarking tool interface. It features a sidebar with navigation options like 'Dashboard', 'New', 'Pipelines', 'Reports', and 'Settings'. The main area displays a table of benchmark runs with columns for 'Run ID', 'Name', 'Duration', 'Triggered by', 'Status', 'Parameters', and 'Run ID'. The table lists several runs, all with a status of 'Completed'.

Run ID	Name	Duration	Triggered by	Status	Parameters	Run ID
10710203-00007-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00007-000	10710203-00007-000
10710203-00008-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00008-000	10710203-00008-000
10710203-00009-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00009-000	10710203-00009-000
10710203-00010-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00010-000	10710203-00010-000
10710203-00011-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00011-000	10710203-00011-000
10710203-00012-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00012-000	10710203-00012-000
10710203-00013-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00013-000	10710203-00013-000
10710203-00014-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00014-000	10710203-00014-000
10710203-00015-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00015-000	10710203-00015-000
10710203-00016-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00016-000	10710203-00016-000
10710203-00017-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00017-000	10710203-00017-000
10710203-00018-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00018-000	10710203-00018-000
10710203-00019-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00019-000	10710203-00019-000
10710203-00020-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00020-000	10710203-00020-000
10710203-00021-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00021-000	10710203-00021-000
10710203-00022-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00022-000	10710203-00022-000
10710203-00023-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00023-000	10710203-00023-000
10710203-00024-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00024-000	10710203-00024-000
10710203-00025-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00025-000	10710203-00025-000
10710203-00026-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00026-000	10710203-00026-000
10710203-00027-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00027-000	10710203-00027-000
10710203-00028-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00028-000	10710203-00028-000
10710203-00029-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00029-000	10710203-00029-000
10710203-00030-000	Import Benchmark Data	1s	Trigger	Completed	10710203-00030-000	10710203-00030-000

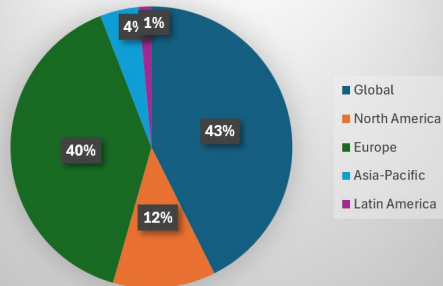
<https://www.youtube.com/watch?v=zF4k0TXCvGw>

brian.glas@owasp.org
owaspsamm.org/benchmarking

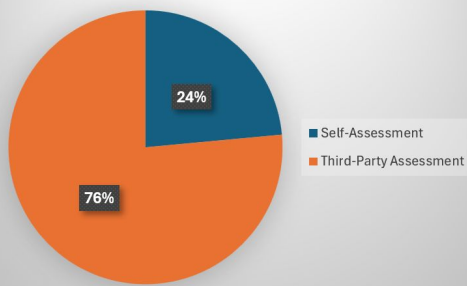


Nov 2025
68 Entries

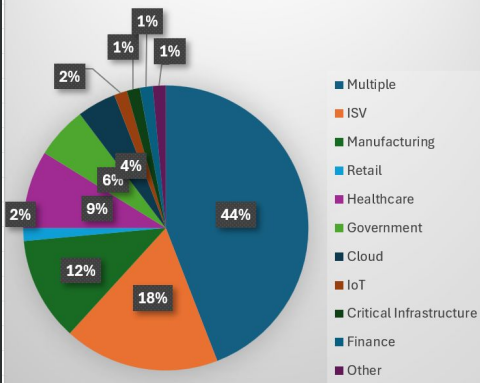
Geographic Region



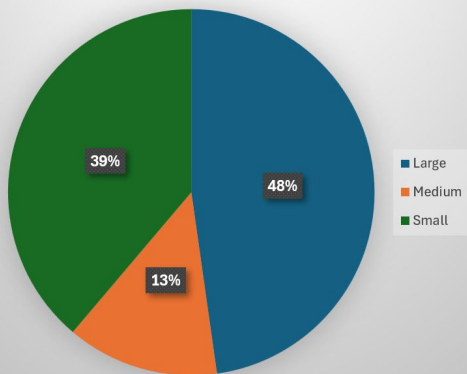
Assessment Type



Industry

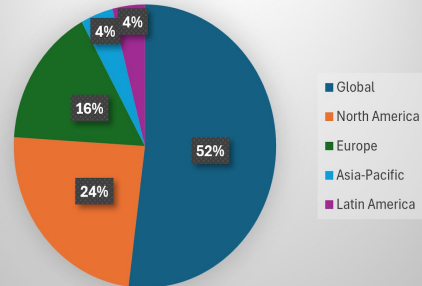


Company Size

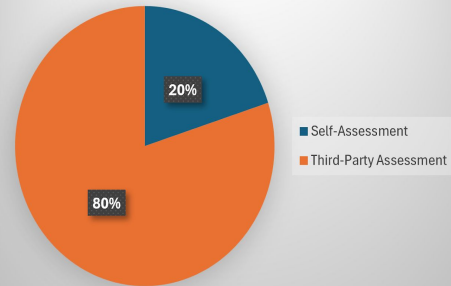


June 2024
25 Entries

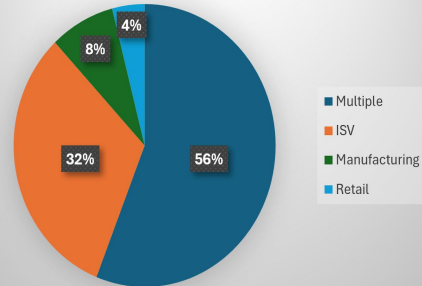
Geographic Region



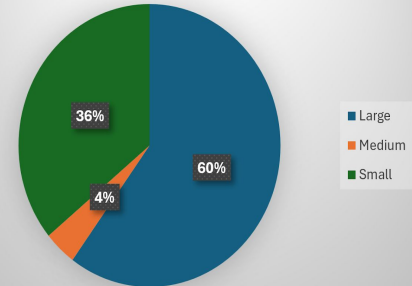
Assessment Type



Industry

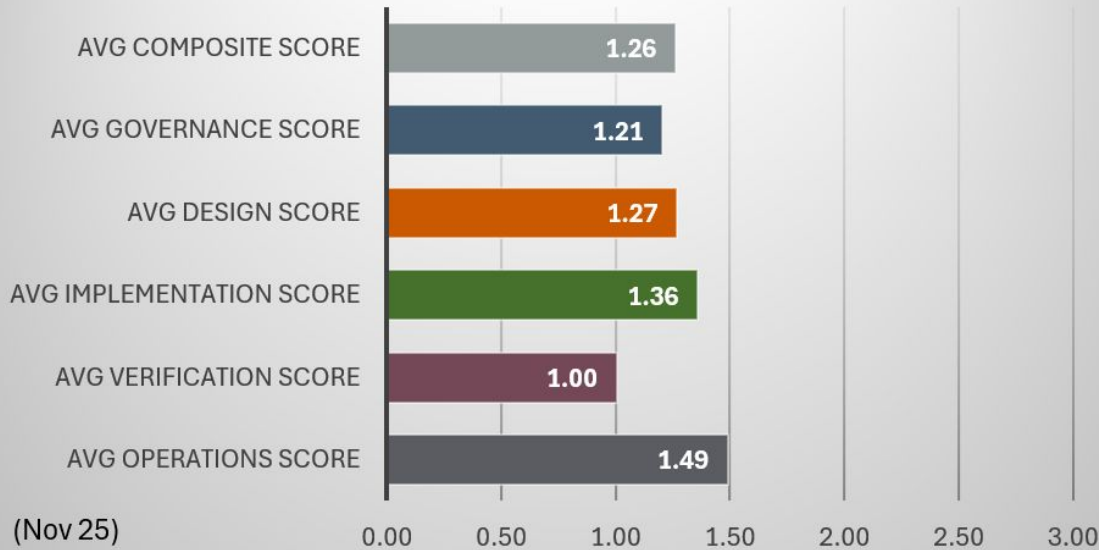


Company Size



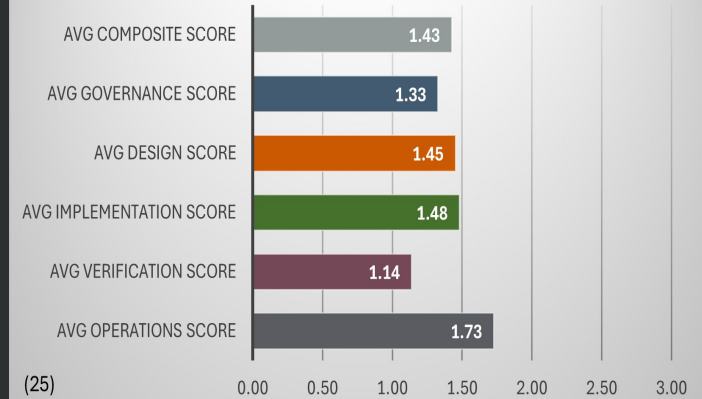
Nov 2025
68 Entries

SAMM Benchmark



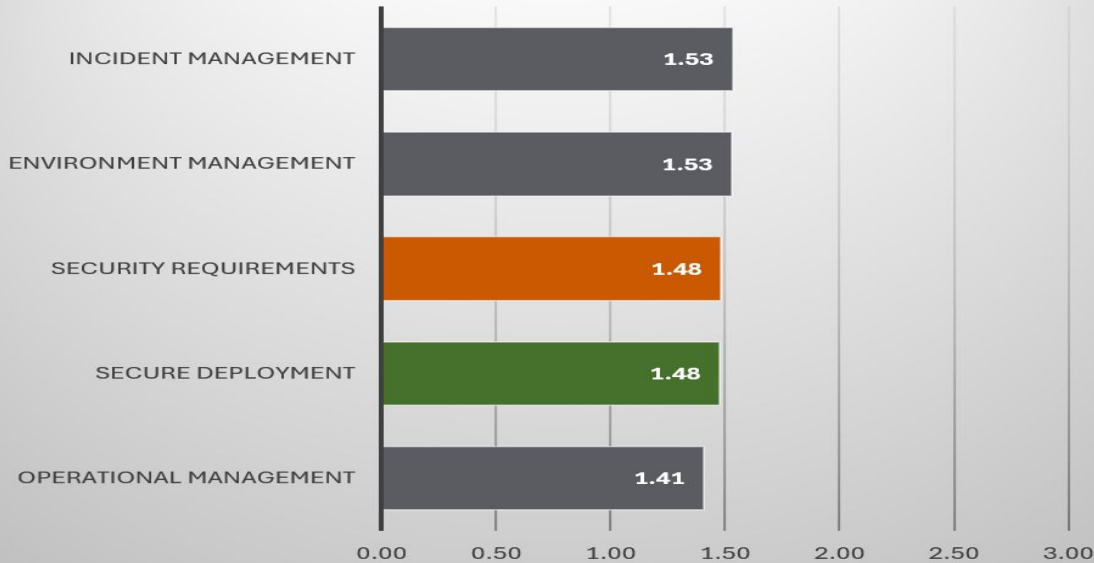
June 2024
25 Entries

SAMM Benchmark June '24



Nov 2025
68 Entries

Top 5 Security Activities



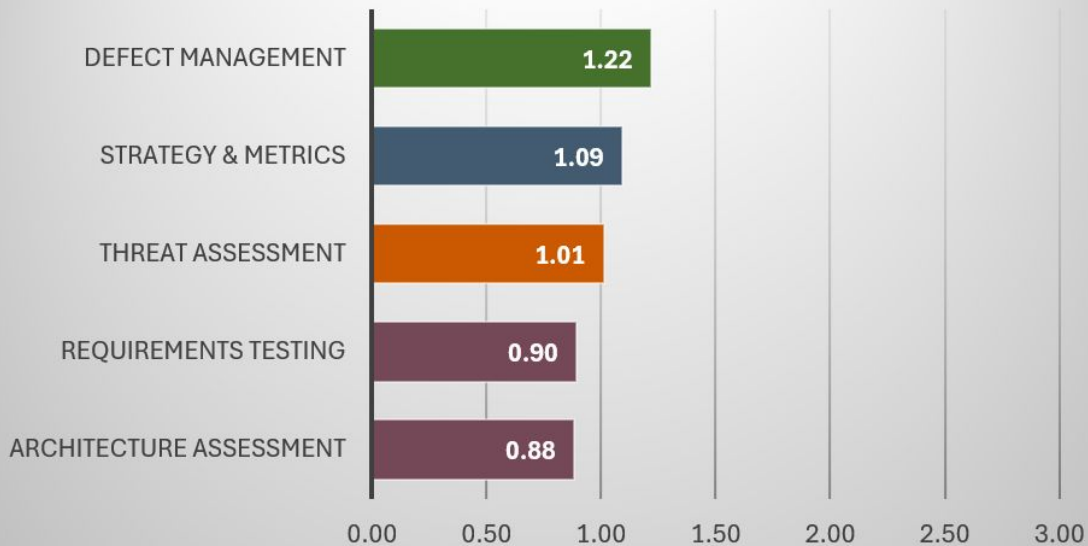
June 2024
25 Entries

Top 5 Security Activities



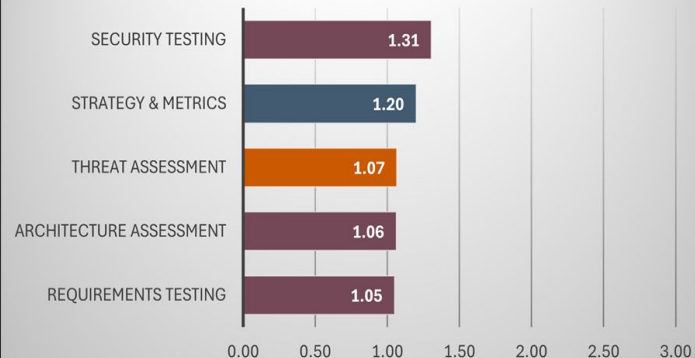
Nov 2025
68 Entries

Bottom 5 Security Activities



June 2024
25 Entries

Bottom 5 Security Activities



Project priorities next 12 months

1. **Make SAMM fit for AI-assisted and AI-generated software development**
2. **Position SAMM as a strong path to CRA-ready secure development**
3. **Strengthen community engagement, visibility, and feedback loops**

Community



Questions

or feedback?





THANK YOU.

[owasp samm.org](https://owasp.org/samm)