



OWASP SAMM ASSESSMENT

Future proof development lifecycle

SECUREHABITS
's-Hertogenbosch, The Netherlands
Document date: 21st August 2026

CONTENTS

Introduction.....	2
About SAMM maturity framework	2
The SAMM Model	2
Benefits	3
Related standards and frameworks.....	3
Our approach	5
Initial consultation.....	5
Assessment	5
Maturity report.....	5
Improvement roadmap	5
Next steps	6
SSDLC policies	6
Implementation of controls	6
Consultants.....	7
Contact Information	8
Contact Information	8
Supplier Information	9
About SECUREHABITS.....	10
Terms and Conditions.....	11

INTRODUCTION

About SAMM maturity framework

In today's fast-paced development environment, ensuring that security is baked into every step of your software development lifecycle (SDLC) is crucial. Our OWASP SAMM SSDLC Maturity Assessment helps software companies identify their current security practices and provides actionable insights to improve and mature their security posture.

The SAMM Model

OWASP SAMM maturity model is divided into five business functions which can be each individually assessed with stake holders responsible for the domain.



Each activity is split into three levels of maturity. First level is expected from all companies, while second and third levels are implemented in more security conscious companies.

During the interview our consultant will explain benefits of each activity and will fill in a special form based on predefined criteria's.

After the assessment you will receive a detailed report which will visually show missing security controls.

In collaboration with our consultants, optionally we can work on prioritization and roadmap for maturity improvement of your organization.

Read more about the OWASP SAMM project here: <https://owaspsamm.org/>

Benefits

Our SSDLC Maturity Assessment helps you identify and close security gaps in your development process, enhancing your overall security posture while aligning with industry standards and regulatory requirements. By integrating security early and throughout the development lifecycle, you'll reduce vulnerabilities, improve software quality, and gain greater confidence in your products' security. This also enables faster, more secure releases, helping you stay competitive and meet your customers' security expectations.

Related standards and frameworks

By using OWASP SAMM you can get ready for the cybersecurity standards and frameworks with specific, measurable and achievable steps.

Below standards and frameworks recommend or require maturing secure development lifecycle:

NIST SP 800-53

Requires secure development practices, particularly in the SA (System and Services Acquisition) family, which includes controls for system development life cycle security.

NIST Cybersecurity Framework (CSF)

Encourages secure development practices under the "Protect" function, particularly in the area of Secure Software Development and Supply Chain Risk Management.

ISO/IEC 27001

Requires the implementation of secure development policies under control A.14.2 (Security in Development and Support Processes).

CIS Controls (Center for Internet Security)

Control 16: Application Software Security, includes requirements for adopting secure development practices in the software development lifecycle.

EU Cyber Résilience Act (CRA)

The EU Cyber Resilience Act mandates the implementation of a secure development lifecycle (SDLC) to ensure that software products and connected devices meet cybersecurity standards throughout their entire lifecycle.

FISMA (Federal Information Security Management Act)

Requires federal agencies to implement security controls, including secure development practices, as part of their risk management and information system security lifecycle.

PCI DSS (Payment Card Industry Data Security Standard)

Version 4.0 includes specific requirements for secure software development, mandating organizations to integrate security throughout the SDLC for payment applications.

Executive Order 14028 (Improving the Nation's Cybersecurity)

This U.S. Executive Order mandates the use of secure development practices for government contractors and agencies, particularly regarding supply chain security and software development.

HIPAA (Health Insurance Portability and Accountability Act)

The HIPAA Security Rule requires covered entities to implement policies and procedures that secure ePHI, which can include secure development lifecycle practices in software handling health data.

CMMC (Cybersecurity Maturity Model Certification)

Requires the implementation of secure development practices at higher maturity levels to protect federal contract information and controlled unclassified information.

FedRAMP (Federal Risk and Authorization Management Program)

Mandates that federal cloud service providers follow secure development practices as part of their overall security controls for government systems.

OUR APPROACH

Initial consultation

To ensure a proper start of the project we initially perform a consultation meeting to define the right scope of assessment. We discuss who would be right stakeholders for each business function.

Once stakeholders are defined we ensure that they are well on boarded and aligned to support the assessment.

Assessment

During the assessment we identify maturity for each of the 15 SAMM activities for the selected scope. Interviewer will take a note or record the session in order to generate a maturity report after this exercise.

Each SAMM activity is divided into three levels of maturity – first one is very basic and expected from all companies. Level two and three are for more security aware organizations.

OWASP SAMM community has a clear description for each activity with acceptance criteria and concrete guideline for implementing them.

Maturity report

After the interview our consultant will prepare a detailed report with notes related to each of the SAMM activity. Client will also receive the overview in a format of graphs and spider web charts for easy consumption of the information.

Improvement roadmap

Our consultants will provide a roadmap recommendation for next steps for maturity improvement for the selected scope. If client requests, few follow up meetings can be performed to have a very detailed and tailored improvement plan with concrete solutions.

Next steps

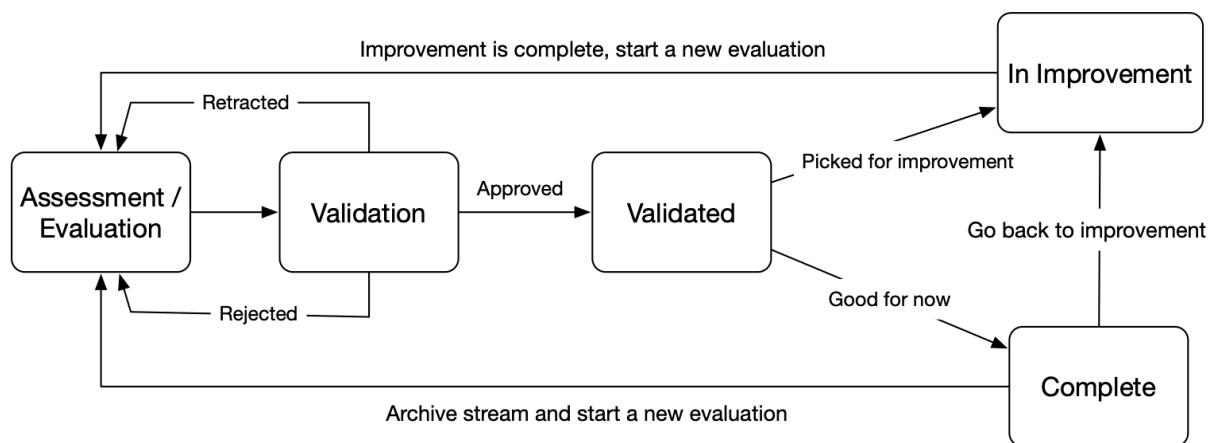
SSDLC policies

Once your internal activities and gaps are known, WiseFrog team can develop and formal SSDLC Policy and SSDLC Whitepaper document that can be publicly shared by your organization with stakeholders. Such documents are very valuable when answering sales RFPs.

Implementation of controls

WiseFrog team can act as a project manager and follow up on the client's maturity improvement initiative. We partner up with the Codific SAMMY and use best tools on the market to ensure success of your program.

Below you can find the business flow we follow to improve each of the 15 SAMM activities:



CONSULTANTS



Nariman Aga-Tagiyev is an Application Security Architect with more than 20 year experience in software development. Have been working as full stack web application developer, backend developer, DevOps engineer, cloud developer and since 2016 fully involved in Application Security related activities.

<https://www.linkedin.com/in/aganariman/>



Eden Yardeni works in application security and is a contributor to OWASP projects, including ASVS v5. She previously worked as a full-stack developer and now focuses on defining and operationalizing application security standards across engineering teams.

<https://www.linkedin.com/in/eden-yardeni/>

CONTACT INFORMATION

CONTACT INFORMATION

We would be happy to have a short call with you to discuss your needs and answer your questions. We do not have aggressive marketing strategy and won't spam you if you get in touch with us.

Contact by email: nariman@securehabits.nl

Contact by phone: [+31655324343](tel:+31655324343)

Schedule a 30 minutes call: <https://securehabits.zohobookings.eu/#/nariman-30m>

SUPPLIER INFORMATION

Company name	SecureHabits
Country of establishment	Netherlands
Address	Willemspoort 102, 5223WV, 's-Hertogenbosch, Netherlands
Email (Invoices)	invoice@securehabits.nl
Email (administrative)	info@securehabits.nl
EU VAT-ID	NL003278436B94
KVK - Dutch Chamber of Commerce number	78029260
IBAN	NL92 ABNA 0876 9924 91
BANK SWIFT (BIC)	ABNANL2A
Contact person	Nariman Aga-Tagiyev
Contact person email	nariman@securehabits.nl
Phone:	+31613732993

ABOUT SECUREHABITS

We offer Application Security Trainings & Consultancy for software development teams.

We are ready to extend your R&D teams with our expertise until your develop in-house skills and habits. Our approach is based on a structural assessment of existing cybersecurity activities with OWASP SAMM Maturity Framework, develop achievable and meaningful roadmap for improvement.

Additionally, we can help you with implementation of the threat modeling, which is a methodical technique for locating and reducing risks in your applications. We can support developers, managers, and security professionals in achieving their security objectives and providing safe software solutions.

TERMS AND CONDITIONS

1. Confidentiality

All information shared by clients during the practical threat modeling training will be treated as confidential. Our trainers are committed to maintaining the privacy and security of any sensitive information provided. This data will not be disclosed, shared, or distributed to any third party outside of the training, except as required by law.

2. Offer Validity

The offer for this practical threat modeling training is valid for a duration of 30 days from the date of issuance. After this period, the offer may be subject to change or withdrawal.

3. Payment Terms

Invoices for the training must be paid within 30 days following the completion of the workshop. Travel costs related to the workshop are not included in the quoted price and will be invoiced separately after the event. Late payments may incur additional charges or penalties as per [Your Company]'s billing policy.

4. Travel Costs

Travel and accommodation costs incurred by trainers for on-site workshops will be billed separately after the workshop. These costs will be outlined in a detailed invoice sent to the client.

5. Cancellation Policy

Cancellations made up to 7 days before the scheduled training date will be eligible for a full refund. Cancellations made within 7 days of the training will not be eligible for a refund. However, substitutions or rescheduling may be allowed with prior notice.

6. Liability

While every effort is made to ensure the accuracy and relevance of the information provided during the training, we are not responsible for any consequences resulting from the use or misuse of the information provided. Clients are responsible for applying threat modeling practices in accordance with their own organizational policies and legal requirements.

7. Intellectual Property

All training materials, including presentations, handouts, and digital resources, remain the intellectual property of SecureHabits. Clients are not permitted to reproduce, distribute, or share these materials outside their organization without prior written consent.