OWASP SAMM

**QUICK START GUIDE**

**OWASP SAMM QUICK START GUIDE**

SAMM (Software Assurance Maturity Model) is the OWASP framework to help organizations assess, formulate and implement a strategy for software security, which can be integrated into their existing Software Development Lifecycle (SDLC). SAMM is fit for most contexts: whether your organization is mainly developing, outsourcing or rather focusing on acquiring software, whether you are using a waterfall or an agile method, the same model can be applied. This quick start guide walks you through the core steps to execute your SAMM-based secure software practice.

**BACKGROUND**

Before diving into actionable steps for a quick start, let’s first briefly describe the model itself. SAMM is based around a set of 12 security practices, which are grouped into 4 business functions. Every security practice contains a set of activities, structured into 3 maturity levels (1 - 3). The activities on a lower maturity level are typically easier to execute and require less formalization than the ones on a higher maturity level. The diagram below illustrates this with example activities found under “Education and Guidance” security practice (which is part of the Governance business function):

**Maturity infographic**

The structure and setup of the **SAMM maturity model** are made to support **(i)** the **assessment** of the current software assurance posture, **(ii)** the definition of the **strategy** (i.e. the target) that the organization should take, **(iii)** the formulation of an implementation **roadmap** of how to get there and **(iv)** prescriptive advice on how to **implement** particular activities. In that sense, the value of **SAMM** lies in providing a means to know where your organization is on its journey towards software assurance, and to understand what is recommended to move to a next level of maturity. Note that **SAMM** does not insist that all organizations achieve maturity level 3 in every category. Indeed, you determine the target maturity level for each “Security Practice” that is the best fit for your organization and its needs. **SAMM** provides a number of templates for typical organizations to this end, but it is recommended that these be adapted to the needs of your organization.

**HOW TO APPLY?**

The diagram below illustrates the typical approach of using **SAMM** in an organization, starting with preparation, going through assessment, setting the target, planning, implementation to roll-out. **SAMM** is particularly well suited to support continuous improvement, in which case the cycle is executed continuously (typically in periods of 3 to 12 months). Note that it is not necessary to always execute all these steps though. **SAMM** could be used to perform just the assessment, or to only define the long-term goals for instance.

**Infographic**

So how do you go about executing the different steps described above? To get started, the following table provides more information for each step in terms of the goal, the different activities to be executed and the most important supporting resources.

**Board**

As part of a quick start effort, the first four phases (preparation, assess, setting the target and defining the plan) can be executed by a single person in a limited amount of time (1 to 2 days). Making sure that this is supported in the organization, as well as the implementation and roll-out phases typically require much more time to execute.

**OWASP RESOURCES**

**The following SAMM resources are referenced in the SAMM Quick Start Guide:**

**• SAMM wiki: https://www.owasp.org/index.php/OWASP\_SAMM\_Project**

**• SAMM downloads:** **https://www.owasp.org/index.php/OWASP\_SAMM\_Project#tab=Downloads**

**• SAMM toolbox:** **https://www.owasp.org/index.php/OWASP\_SAMM\_Project#tab=Downloads**

**• Browse SAMM online:** **https://www.owasp.org/index.php/OWASP\_SAMM\_Project#tab=Browse\_Online**

**• SAMM project plan template:** **https://www.owasp.org/index.php/OWASP\_SAMM\_Project#tab=Downloads**

**• OWASP resources: https://www.owasp.org/index.php/Main\_Page**

To apply SAMM you will find a lot of great resources at OWASP. We have created a SAMM resources collection on the OWASP wiki.

Go to **https://www.owasp.org/index.php/SAMM-Resources** to discover all our SAMM Resource online.

This wiki category links OWASP and other resources to SAMM Security practices.

FINAL NOTES

The best way to grasp SAMM is to start using it. his document has presented a number of concrete steps and supportive material to execute on. Now it’s your turn. We warmly invite you to spend a day or two on following the first steps, and you will quickly understand and appreciate the added value of the model. Enjoy!

Suggestions for improvements are very welcome. And if you’re interested, consider to join the mailinglist or become part of the SAMM community.

**Discover SAMM online - https://www.owasp.org/index.php/SAMM**

**Subscribe to our SAMM mailing list - https://lists.owasp.org/mailman/listinfo/samm**

**Follow us on Twitter - https://twitter.com/OwaspSAMM**