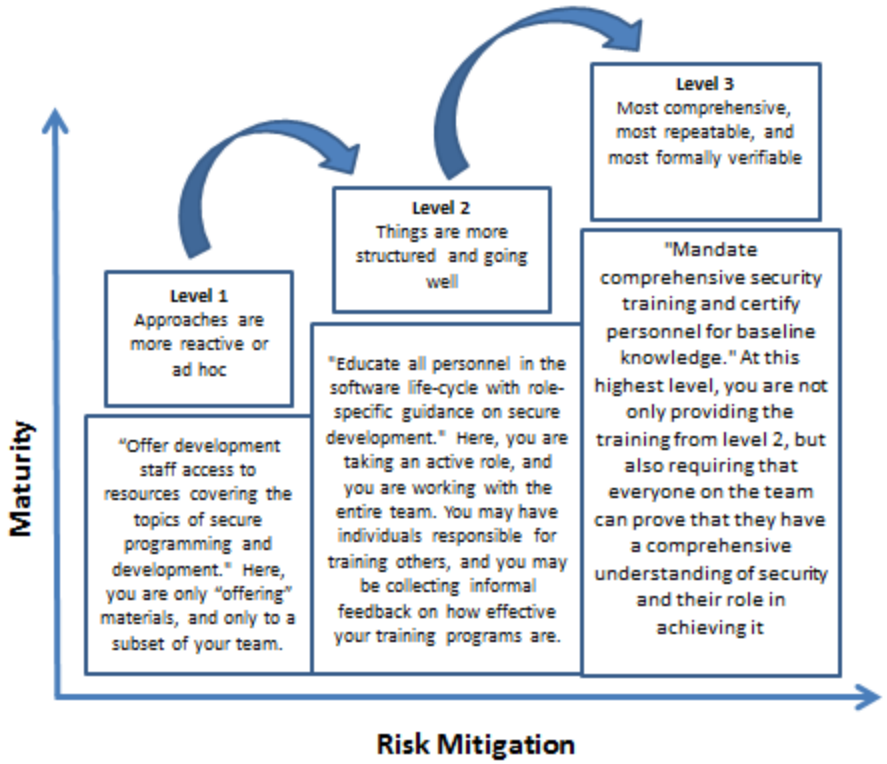
OWASP SAMM Quick Start Guide

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 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

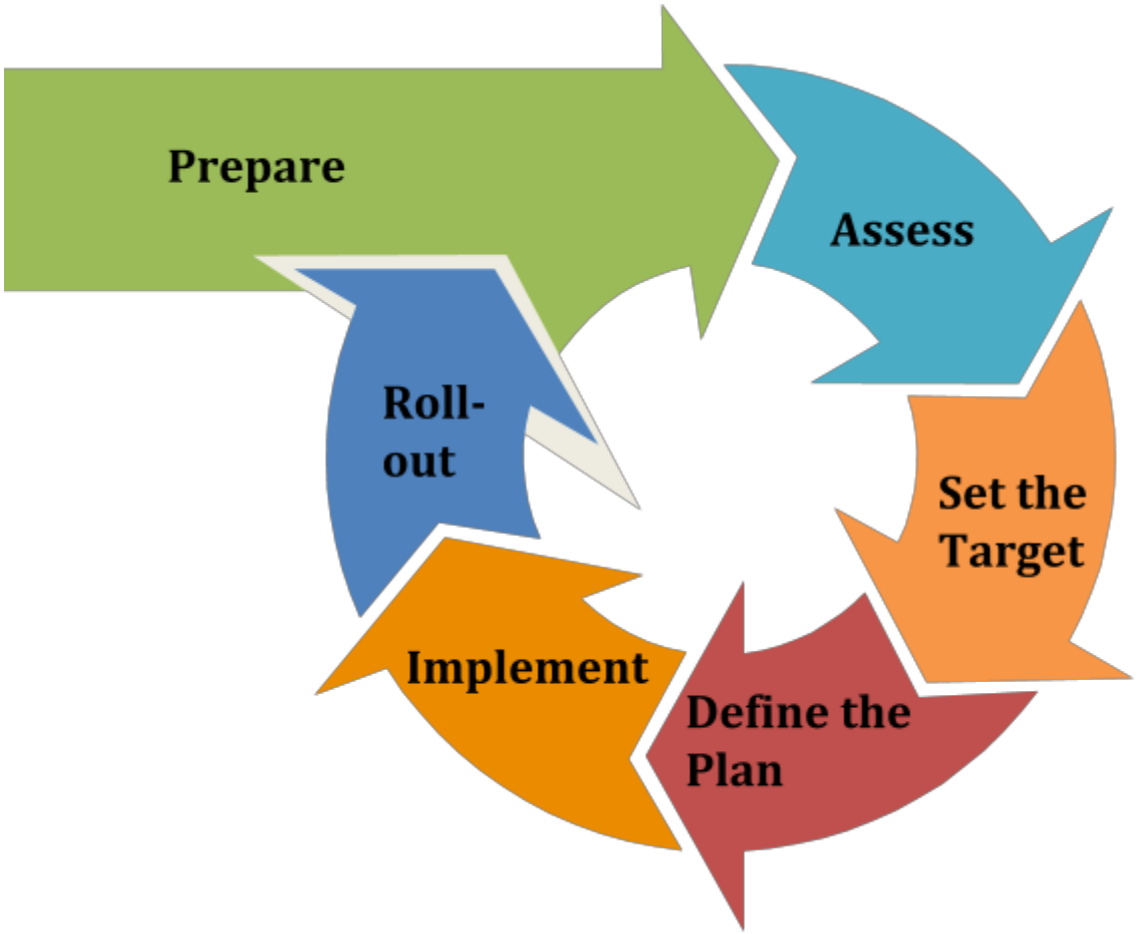
Before diving into actionable steps for a quick start, let's first briefly discuss the model itself. SAMM is based around a set of 12 security practices, which are grouped into 4 business functions. Every security practice contains a set of activities, structured into 3 maturity levels (1 – 3). The activities 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 the under "Education and Guidance" security practice (which is part of the Governance business function):



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 is providing a means to knowing where your organization is on its journey towards software assurance, and to understanding 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 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 you can adapt these as you see fit.

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.



So how do you go about executing the different steps described above? Well, as they say, the proof of the pudding is in the eating. For you to get started, the following table provides for each step more information in terms of the goal, the different activities to be executed and the most important supporting resources.

Step	Purpose	Activities	Resources	Best Practices
Prepare	Ensure a proper start of the project	*Define the scope* Set the target of the effort: the entire enterprise, a particular application or project, a particular team … *Identify stakeholders* Ensure that important stakeholders to support and execute the project are identified and well aligned. *Spread the word* Inform people about the initiative and provide them with information to understand what you will be doing	Consider involving at least: • Executive Sponsor • Security Team • Developers • Architects • Business Owners • QA Testers • Managers The OpenSAMM main site: http://www.opensamm.org/ The model in .pdf: http://www.opensamm.org/downloads/SAMM-1.0.pdf	Pre-screen software development maturity to have realistic expectations
Assess	Identify and understand the maturity of your chosen scope in each of the 12 software security practices	*Evaluate current practices* Organize interviews with relevant stakeholders to understand the current state of practice within your organization. You could evaluate this yourself if you understand the organization sufficiently well. SAMM provides lightweight and full assessments (where the latter is an evidence-based evaluation) – use the full	The OpenSAMM toolbox (TODO: include link here) Online Self Assessment Tool https://ssa.asteriskinfosec.com.au Both of these resources provide you with:	Ensure consistent assessment for different stakeholders and teams by using the same questions and interviewer Consider using different formats to gather data (e.g., workshops vs. interviews)

		only if you want to have absolute certainty about the scores. *Determine maturity level* Based on the outcome of the previous activity, determine for each security practice the maturity level according to the SAMM maturity scoring system. In a nutshell, when all activities below and within a maturity level have been implemented, this level can be used for the overall score. When extra higher-level activities have been implemented without reaching a full next level, add a "+" to the rating.	• assessment questions • maturity level calculation	Ensure interviewees understand the particularities of activities Understand which activities are not applicable to an organization and take this into account in the overall scoring Anticipate/document whether you plan to award partial credit, or just document various judgement calls Repeat questions to several people to improve the assessment quality Consider making interviews anonymous to ensure honesty *Take questions not too literally*
Set the Target	Develop a target score that you can use as a measuring stick to guide you to act on the "most important" activities for your situation	*Define the target* Set or update the target by identifying which activities your organization should implement ideally. Typically this will include more lower-level than higher-level activities. Predefined roadmap templates can be used as a source for inspiration. Ensure that the total set of selected activities makes sense and take into account dependencies between activities. *Estimate overall impact* Estimate the impact of the chosen target on the organization. Try to express in	Predefined templates See the book Software Assurance Maturity Model (SAMM) Roadmap Chart Worksheet http://www.opensamm.org/downloads/resources/20090610-Samm-roadmap-chart-template.xls Project 71 as a comparative source	Take into account the organisation's risk profile Respect dependencies between activities The overall impact of a software assurance effort is estimated at 5 to 10% of the total development cost.

		budgetary arguments. SAMM provides initial metrics in this direction.		
Define the Plan	Develop or update your plan to take your organization to the next level	*Determine change schedule* Choose a realistic change strategy in terms of number and duration of phases. A typical roadmap consists of 4-6 phases of 3 to 12 months. *Develop/update the roadmap plan* Distribute the implementation of lacking activities over the different roadmap phases, taking into account the effort required to implement them.. Try to balance the implementation effort over the different periods, and take into account dependencies between activities.	Software Assurance Maturity Model : A guide to building security into software development page 33 http://www.opensamm.org/downloads/SAMM-1.0-en_US.pdf Project Plan http://www.opensamm.org/downloads/resources/20090615-SAMMProject.zip	Identify quick wins and plan them early on Start with awareness/training Adapt to coming release cycles / key projects
Implement	Work the plan	*Implement activities* Implement all activities that are part of this period. Consider their impact on processes, people, knowledge and tools. The SAMM model contains prescriptive advice on how to do this. OWASP projects may help to facilitate this.	Useful OWASP resources per activity are described at https://www.owasp.org/index.php/Category:SAMM-Resources	Treat legacy software separately. Do not mandate migration unless really important. Avoid operational bottle-necks (in particular for the security team)
Roll-out	Ensure that improvements are available and effectively used within the organization	*Evangelize improvements* Make sure people are aware of the implemented improvements by organizing trainings and communicating.		Categorize applications according to their impact on the organization. Focus on high-impact applications.

		Measure effectiveness Measure the adoption and effectiveness of implemented improvements by analyzing frequency and impact.		Use team champions to spread new activities throughout the organization

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.

Final notes

The best way to grasp SAMM is to start using it. This document has presented a number of concrete steps and supportive material to execute these. 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. Good luck !