Open SAMM Quick Start Guide

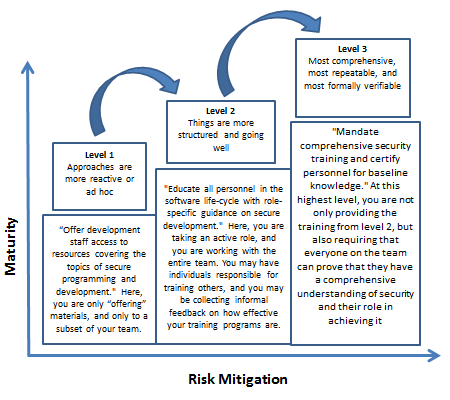
Open SAMM (Software Assurance Maturity Model) is an open framework designed to help organizations understand and improve the security-related aspects of their software development lifecycle. Like any new framework, it can be difficult to absorb all at once. The best way to develop an understanding of SAMM is to try it out.

This quickstart guide helps you do that.

SAMM provides a way to measure how well your organization can reliably produce secure software. It provides a way to identify strong areas, weak areas, and a map to help get your organization to the next level in four key areas, which SAMM calls "business functions":

Each of these "business functions" is further broken down into "Security Practices" that contain activities that are recommended to achieve a certain level of maturity in that particular “business function”.

As an illustration, these are the maturity levels found under "Education and Guidance":

****

Knowing where your organization is on its journey and what is recommended to move tothe next level of maturity is the value of Open SAMM

Perhaps the most important thing to know about SAMM, though, is that it does not insist that all organizations should achieve level 3 in every category. It simply offers an objective 4-step framework for assessing your maturity level:

SAMM provides clear evaluation criteria so that an organization may make concrete plans to achieve the next level. Those same criteria can also support a decision not to pursue the next level in a given area. In some cases, the extra administrative burden that comes with level 3 may be more than your organization is ready to accept.

You determine the level of each “Security Practice” that is the best fit for your organization and its needs.

**Start Your Journey Here:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Task** | **Purpose** | **Tool Available** | **Estimated Time Requirement** |
| 1 | Understand the Framework | Gain a high level overview of the framework and | Software Assurance Maturity Model  <http://www.opensamm.org/downloads/SAMM-1.0.pdf>  Presentations, tools and the documentation translations  <http://www.opensamm.org/download/> | 30 minutes |
| 2 | Conduct a Self Assessment | See if you have all the proper processes and procedures in place and determine how mature they are. | Software Assurance Maturity Model : A guide to building security into software development page 19  <http://www.opensamm.org/downloads/SAMM-1.0-en_US.pdf>  Open SAMM Assessment Worksheet  <http://www.opensamm.org/downloads/resources/20090925-SAMM-Assessment-v0.4.xls>  Software Assurance Maturity Model (SAMM) Interview Template  <http://www.opensamm.org/downloads/resources/20090607-SAMMAssessmentInterviewTemplate-1.0.xls> | 20 minutes |
| 3 | Pick or develop a Scorecard | Since all industries are different and have different needs develop a score card that you can use as a measuring stick to guide you to act on the “most important” processes and procedures for your situation. | Software Assurance Maturity Model : A guide to building security into software development page 26  <http://www.opensamm.org/downloads/SAMM-1.0-en_US.pdf>  Software Assurance Maturity Model (SAMM) Roadmap Chart Template  <http://www.opensamm.org/downloads/resources/20090610-Samm-roadmap-chart-template.xls> | 30 minutes |
| 4 | Develop a Plan | Develop your individual plan to take your organization to the next level | 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> | 1 hour |
| 5 | Implement the plan and return to Step 2 | Work the plan and remeasure to see if you have matured. | OWASP Documentation and Tools | Depends on task complexity |