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 and weak areas, and provides a map towards improvement in four key areas, which SAMM calls "business functions":

Governance: how well are your goals defined and communicated?

Construction: how do you decide what to build?

Verification: how do you know you built what you intended to build?

Deployment: how do you manage things after a release?

Each of those four areas is comprised of three specific categories, which SAMM calls "Security Practices." For example, the "Governance" function includes these three:

Strategy and Metrics: Generally speaking, where do you want to go, and how will you know when you're getting there?

Policy and Compliance: What are the specific rules you will follow, and how will you make sure you're actually following them?

Education and Guidance: How will you teach your staff what's expected of them? What resources will you provide?

It is at the bottom level - these "Security Practices" where SAMM provides measurement criteria to sort processes into one of three "maturity levels." A level 1 approach is more reactive or ad hoc, level 2 is where things are more structured and going well, and level 3 is the most comprehensive, most repeatable, and most formally verifiable.

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

Level 1: "offer development staff access to resources covering the topics of secure programming and development." Here, you are only "offering" materials, and only to a subset of your team.

Level 2: "Educate all personnel in the software life-cycle with role-specific guidance on secure development." Here, you are taking an active role, and you are working with the entire team. You may

have individuals responsible for training others, and you may be collecting informal feedback on how effective your training programs are.

Level 3: "Mandate comprehensive security training and certify personnel for baseline knowledge." At this highest level, you are not only providing the training from level 2, but also requiring that everyone on the team can prove that they have a comprehensive understanding of security and their role in achieving it.

The other areas include similar categories, which are clearly outlined in the rest of the materials about 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:

Step 1: Measure current levels.

Step 2: Decide where gaps exist, and at what level you'd like to rate in each area at the next assessment.

Step 3: Make concrete plans to close the gaps.

Step 4: Implement those plans, then return to step 1.

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.

Next Steps:

In order to see what you can gain from SAMM, we recommend that you do a simple exercise, on your own or with a very small group, to gauge your current maturity level in each of the four Business Functions. SAMM makes this initial assessment very easy, by providing just two or three "yes/no" questions for each of the 12 Security Practices. An Excel workbook is available which does the calculations for you, based on these simple yes/no answers.

When you've completed that exercise, and you have a general idea of where your organization falls on each of the measurements, ask yourself if your current maturity level is where you want it to be in each area.

Read through the descriptions of any areas where there is a gap, and use the materials to develop plans to close those gaps over time.