BSIMM

Building Security In
Maturity Model

Everything You Need to Know About BSIMM

Answers to Your Most Frequently Asked Questions

by BSIMM experts Sammy Migues and Paco Hope

Defining BSIMM Principles

Q What's the difference between OpenSAMM and BSIMM?

A The two key differences are 1) descriptive vs. prescriptive and 2) the BSIMM community.

While both **OpenSAMM** (Software Security Maturity Model) and **BSIMM** (Building Security In Maturity Model) are built from considerable software security experience, BSIMM is descriptive, not prescriptive. It documents what firms actually do, not necessarily what a small group of security experts think they ought to do. Built from hundreds of assessments in more than 200 companies, BSIMM is a living model that is regularly updated to reflect actual practices in real software security initiatives (SSIs). The changes to BSIMM happen because changes in actual software development practices happen.

OpenSAMM was created in 2008 as a prescriptive framework that tells firms what they should do. While built by experienced experts, it is a generic framework based on reasonable ideas. BSIMM, by contrast, is based on things that firms actually do. If there is something listed as an activity in BSIMM, there are several (sometimes dozens) of real firms that are actually doing that activity, and they have confirmed fairly recently that they still do it. If firms do not spend considerable effort doing an activity, it does not appear in the BSIMM. In some sense, OpenSAMM represents a small group's wish list of activities for software development, whereas BSIMM represents a documentary approach that records what is actually happening.

BSIMM is based on things that firms actually do.

BSIMM also has an active community that includes mailing lists and twice yearly global conferences. This enables firms who measure their initiatives with BSIMM to learn from each other and collaborate to improve their SSIs. OpenSAMM community events are rare and focus on building OpenSAMM itself, not improving the capabilities of SSIs.

Q What could constitute an open source risk? How do I identify open source risk?

A The **bad outcomes associated with using open source software** are numerous, for example:

- Open source can include licensing issues, such as when **Cisco settled a law suit related to Linksys's use of GNU Public License (GPL) source code**.
- Open source components can be out of date or can have known vulnerabilities.
- If open source software is included in an application, vulnerabilities in the open source components become vulnerabilities in the application itself.
- There may not be anyone to report bugs to in open source and making a critical bug public may put thousands of

other firms at risk.

- If open source projects are abandoned by their core developers, a firm that relies on an open source component can find itself forced to maintain code they didn't write to keep it current with best practices.
- Firms often require development teams to identify all open source components used in any products and services that are sold.
- Legal teams often review the licensing terms for those components to ensure the terms are compatible with the firm's use of the open source component.

The list goes on, which makes identifying a **complete list of open source software risks** beyond the scope of this FAQ.

Q As we know, 'no one way to eat the banana' is the best way. So how are the security activity levels of maturity categorized?

A Within each practice, activities are assigned to levels based primarily on their observation frequency. The most rarely observed practices are generally found in the most mature SSIs, and the most commonly observed practices are generally found in all SSIs. We used mathematical methods to draw these boundaries and then checked and confirmed that they were appropriate using our experience.

Q SSG vs. Satellite: Are the satellite people usually SSG people embedded within product teams or are they more commonly product team engineers who are security savvy?

A The SSG is usually not part of a product team or business unit. The SSG is usually a central team of people at a group level that have a broad software security remit. Generally, the satellite is a set of people who are not central, but who focus on security within a narrower context, such as a business unit or application team. They are interested and engaged developers, architects, software managers, testers, and similar roles who have a natural affinity for software security and are organized and leveraged by a SSI.

Q You mentioned that security is an emergent property of the system. Could you elaborate on how that principle impacts BSIMM?

A Security as a property "emerges" from the successful execution and interaction of many activities in the software lifecycle. An appropriate mix of BSIMM activities in a firm's SSI will help ensure that the emergent property "security" is appropriate for each piece of software in the firm's portfolio. On the other hand, firms that attempt to execute *every* activity listed in BSIMM would be doing themselves a disservice and not necessarily achieving secure software as a result.

This emergent nature stands in contrast to a checklist mentality, which suggests that when all activities are executed, all jobs are done and the result must be secure simply because the process was followed. Finally, there is no amount of testing done at the end of a development cycle that puts "security" into broken software.

> There is no amount of testing done at the end of a development cycle that puts "security" into broken software.

Q Do BSIMM practices vary by the type of group/product? For example, embedded software vs. IT application software?

A In a word: No. BSIMM activities have been used to measure SSIs in firms of all shapes and sizes in many different vertical markets producing software for many different target environments. Naturally, implementation of an activity will vary across firms and possibly for different groups within a single firm, but the activity remains the same.

One might ask: do car mechanics do different things based on the model of car (e.g., delivery van, sports car, personal car)? The answer is sort of yes and sort of no. Do they use different tools? Again, sort of yes and sort of no. BSIMM is looking at broad-level activities like whether the oil is changed regularly, not specific things like whether the oil is changed based on time versus mileage, the size of the oil filter, or whether it's regular versus synthetic oil.

Q How are BSIMM measures defined, e.g an activity is no longer performed?

A If a firm is measured and they are currently performing an activity, their score reflects that activity currently occurring. If they are measured again, some months or years later, and the activity is not occurring at that time, their BSIMM score will reflect that. There is no ongoing verification of activities occurring.

Implementing a BSIMM

Q What does the BSIMM process entail?

A A typical BSIMM assessment involves a team of two or three assessors interviewing about 15-20 people over the course of a couple days. Interviews are usually no more than 1.5-2 hours each. Assessors look at some artifacts (documents, etc.), as required. Assessors don't need any more access or support than any other visitor to your office might need. No one interacts with applications or data. It's about the software process, not the application or the data. BSIMMs result in a written report, a discussion of the results, and recommendations for additional efforts.

Because the BSIMM itself is scientific, we try to stay close to the data. That is, we report on what is present and what is not present and we compare it to what we've seen in other places. A BSIMM report always highlights areas where there are significant differences between typical SSIs and the subject SSI. We always point out areas where we think additional effort may yield beneficial results.

Q For large organizations with many products, is it better to analyze each product or review the organization as a whole?

A BSIMM is used to assess SSIs (aka application security programs), not individual development projects. There is usually benefit to measuring individual business units as well as overall enterprise capabilities. However, for small- to mid-sized firms that have only a single security group, a single BSIMM measurement is the right answer.

Q Is there any prescribed frequency for assessments?

A As always, BSIMM doesn't prescribe or recommend anything. We observe and report. The current average in the BSIMM community is about 22 months between a first and second assessment. Several organizations do BSIMM assessments more frequently. Some firms have used a BSIMM measurement to kick off a one- or two-year effort to make demonstrable improvements in their SSI. They remeasure after one or two years to assess the result of their efforts.

Q When you break down groups in a large organization to be measured separately, how is it typically done?

A Large organizations typically perform an assessment of the central SSG, then within each major business unit. Sometimes technology boundaries and business boundaries are similar (e.g., one business unit is responsible for back-end systems, another for mobile apps), but BSIMM is typically aligned on business boundaries (i.e., the remit of the security team being assessed is the scope of BSIMM).

Q Is there a downloadable template version of your assessment tool?

A There isn't an assessment tool in the traditional sense such as an interactive site or tool that asks you questions and determines a score from your answer. If you want to self-assess, your best bet is to read the **BSIMM report**. It contains details about each of the 112 activities which you can use to estimate your own maturity or periodically chart your initiative's progress over time.

Interpreting BSIMM Results

Q Why does my company need a maturity model?

A A BSIMM measurement gives you a concrete score of the current state of your SSI and a way to gauge its progress over time.

Q How should/could the data from the evaluation be interpreted?

A BSIMM is a bit like a thermometer. Thermometers tell you how hot or cold something is, but firms making ice cream and firms making hamburgers don't want to be the same temperature. One key way firms interpret a BSIMM measurement is by comparing what practices are possible versus which ones they are doing. It's often the case that specific areas of the software security framework (e.g., SDLC Touchpoints, Configuration Management, and Vulnerability Management, etc.) will stand out as areas that are important to the firm's business objectives and also as areas that are lacking in activity.

Q Is BSIMM best looked at as a benchmarking of security capabilities against other organizations or benchmarking against standard practices?

A A BSIMM assessment is more like a repeatable way to perform an inventory of software security activities as defined by a standardized model. BSIMM data show the observation rate for each of the activities, providing insight into how many other organizations think an activity is important and applicable.

Q Does the model measure effectiveness? How do you rate the efficacy of a particular practice?

A No, BSIMM does not evaluate how effective a firm's practice is. For example, a firm could use a tool to perform regular scans of an application, regular static analysis of source code, or some other activity. And they could have the tool configured in a way that misses some defective types. BSIMM might give them credit for performing the activity. A firm does not have to do something to a certain level of effectiveness in order to get credit for doing it. Having said this, virtually no Level 2 or Level 3 maturity activities can be achieved by simply showing up.

Q Just because a lot of firms do it, doesn't mean it's effective, right? I mean, if 90 out of 100 people eat candy, it doesn't mean they should!

A Yes and no. An implicit assumption to BSIMM is that firms will change what they do over time because they will discover through experience what works and what doesn't work. The BSIMM model has changed over time to include new activities that weren't seen in earlier years.

While that observation might be true for candy, software security activities take significant amounts of time and money from a CISO's limited budget. It's doubtful that activities observed very frequently are done just for grins. It's reasonable to use prevalence as a proxy for utility. We believe

It's reasonable to use prevalence as a proxy for utility.

that through repeat measurements and the active nature of the community, the model will adjust automatically. If an activity is popular today, but it turns out to be ineffective, we will see the community pivot away from it and we will stop observing it. It will drop from the model and we will stop reporting on it.

Industry-specific questions

Q Why don't any government agencies get BSIMM measured?

A There is no particular reason. More than 200 organizations have been measured so far. There is nothing preventing or inhibiting public sector agencies from being measured.

Q Is there a breakdown of the 10 healthcare companies by their numbers (e.g. "Number of SSG members per dev.") available somewhere?

A Not currently. We may provide such data when there are more firms in the group.

Q Has the DHS, DISA, and/or the DoD expressed an interest in implementing BISMM into their requirements (e.g. RMF/NIST)

A No.

About the vBSIMM

Q Is it appropriate to ask my vendors about their security program? Is there some measurement model we could ask to see for their programs?

A It's not just appropriate, it's a really good idea. Software risk comes from many sources, including vendors of products and services that a firm uses. There are two approaches we have seen taken: **vBSIMM (BSIMM for vendors)** and BSIMM itself. The vBSIMM is lightweight and suitable for doing fast, repeatable measures of large numbers of vendors. When a firm has a small number of vendors, the firm can encourage or require them to measure their own initiative via BSIMM.

Q Should vBSIMM happen in parallel with BSIMM?

A It can. Whether that is a good idea depends on the ability of the firm to consume the output of both activities simultaneously. Typically, a firm measures itself first to get comfortable with the measurement and to understand its implications. Measuring vendors is usually done afterwards and separately.

Q Is there a new version of vBSIMM forthcoming? Where can the latest version be obtained?

A The latest version of vBSIMM can be found at **https://www.bsimm.com/about/bsimm-for-vendors/.**

About BSIMM

The **Building Security In Maturity Model (BSIMM)** is a study of existing software security initiatives. By quantifying the practices of many different organizations, we can describe the common ground shared by many as well as the variation that makes each unique. BSIMM is not a "how to" guide, nor is it a one-size-fits-all prescription. Instead, BSIMM is a reflection of software security.

Learn more at **https://www.bsimm.com/**.