BSIMM

Everything You Need to Know About the BSIMM

Answers to Your Most Frequently Asked Questions

by BSIMM expert Sammy Migues

Defining BSIMM principles

QUESTION:

What's the difference between the OpenSAMM and the BSIMM?

ANSWER:

Two of the many differences are (1) descriptive versus prescriptive and (2) the BSIMM community.

While both the OpenSAMM (Software Assurance Maturity Model) and the **BSIMM** (Building Security In Maturity Model) are built from considerable software security experience, the 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 160 companies, the BSIMM is a living model that is regularly updated to reflect actual practices in real software security initiatives (SSIs). Changes to the BSIMM happen because changes in actual software development practices happen.

> The BSIMM is based on things that firms actually do.

The 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. Also started in 2008, the BSIMM, by contrast, is based on things that firms actually do. If something is listed as an activity in the 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, the OpenSAMM represents a small group's wish list of activities for software development, whereas the BSIMM represents a documentary approach that records what is actually happening.

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

QUESTION:

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

ANSWER:

The bad outcomes associated with unknowingly or inappropriately using open source software are numerous:

- Open source can have licensing issues, such as when Cisco settled a lawsuit related to Linksys' use of GNU Public License (GPL) source code.
- Open source components can be out-of-date or 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 for open source software, and making a critical bug public may put thousands of other firms at risk.
- If open source projects are abandoned by their core developers, firms that rely on an open source component can find themselves forced to maintain code they didn't write to keep it current with best practices.

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

Software composition analysis that properly inventories and reports vulnerabilities in all open source use within a firm is the first step to good open source risk management.

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

QUESTION:

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

ANSWER:

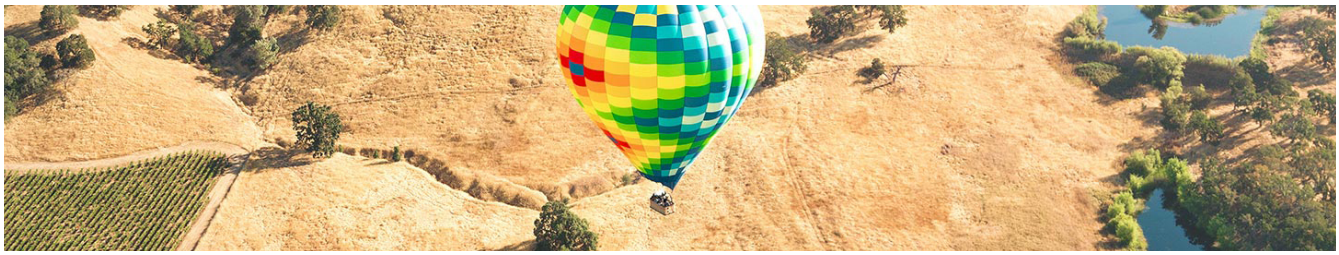
Within each practice, activities are assigned to levels based primarily on their observation frequency. The most rarely observed practices are generally found in the most mature SSIs, and the most commonly observed practices are generally found in all SSIs. We use mathematical methods to draw these boundaries.

QUESTION:

SSG versus satellite: Are the satellite people usually SSG people embedded within product teams, or are they more commonly product team engineers who are security savvy?

ANSWER:

The software security group (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 and are not part of the SSG. They generally are members of the engineering teams 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 by and contribute to an SSI.



QUESTION:

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

ANSWER:

Security as a property emerges from the successful execution and interaction of many activities in the software life cycle. 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.

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. Firms that attempt to execute every activity listed in the BSIMM are doing themselves a disservice and not necessarily achieving secure software as a result.

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

QUESTION:

Do BSIMM practices vary by the type of group/product—for example, embedded software versus IT application software?

ANSWER:

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 vehicle (e.g., delivery van, sports car, family car)? Do they use different tools? When we think in terms of whether the tires are rotated regularly, the fluids are changed periodically, and the vehicle is inspected by a qualified technician, then the make and model of the car affects only the execution details, not the activities. The BSIMM looks at broad-level activities like whether the oil is changed regularly, not specific things like whether the oil is changed based on time or mileage, the size of the oil filter, or whether it's regular or synthetic oil.

QUESTION:

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

ANSWER:

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

Implementing the BSIMM

QUESTION:

What does the BSIMM assessment process entail?

ANSWER:

A typical BSIMM assessment involves a team of two or three assessors interviewing about 15–20 people over the course of a couple of 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 an audit of applications or the data. BSIMM assessments 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.

QUESTION:

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

ANSWER:

The BSIMM is used to assess SSIs (a.k.a. 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-size firms that have only a single security group, a single BSIMM measurement is the right answer.

QUESTION:

Is there any prescribed frequency for assessments?

ANSWER:

The BSIMM doesn't prescribe or recommend anything. We observe and report. The current average in the BSIMM community is about 27 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 SSIs. They remeasure after one or two years to demonstrate the results of their efforts.

QUESTION:

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

ANSWER:

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 the BSIMM is typically aligned on business boundaries (i.e., the remit of the security team being assessed is the scope of the BSIMM).

QUESTION:

Is there a downloadable template version of your assessment tool?

ANSWER:

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 116 activities that you can use to estimate your own maturity or periodically chart your initiative's progress over time.

Interpreting BSIMM results

QUESTION:

Why does my company need a maturity model?

ANSWER:
A BSIMM measurement gives you a concrete score regarding the current state of your SSI as well as a way to gauge its progress over time.

QUESTION:

How should/could the data from the assessment be interpreted?

ANSWER:
The 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 their products 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., software development life cycle touchpoints, configuration management, vulnerability management, vendor management, training) will stand out as areas that are important to the firm's business objectives and also lacking in effort.

QUESTION:

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

ANSWER:

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.

QUESTION:

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

ANSWER:

No, the 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, but the tool could be configured in such a way that it misses some defect types. The BSIMM might give the firm credit for performing the testing activity because it is being performed. A firm does not have to do something to a certain level of effectiveness to get credit for doing it. That said, virtually no Level 2 or Level 3 maturity activities can be achieved by simply buying a tool and using it improperly.

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

QUESTION:

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!

ANSWER:

Yes and no. An implicit assumption in the BSIMM is that firms will change what they do over time because they will discover through experience what works and what doesn't work for them. 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 that through repeat measurements and the active nature of the community, the model will adjust automatically. If an activity is popular today but 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

QUESTION:

Why don't any government agencies get BSIMM assessments?

ANSWER:

There is no particular reason. More than 160 organizations have been measured so far. There is nothing preventing or inhibiting public sector agencies from being measured. That said, a BSIMM assessment measures a software security initiative, so you need to have an SSI before you get a BSIMM assessment.

QUESTION:

Has the DHS, DISA, or DoD expressed an interest in implementing the BSIMM in their requirements (e.g., RMF/NIST)?

ANSWER:

No one has called and asked about it that way. On the other hand, the BSIMM is licensed through Creative Commons, so they are free to use it with attribution.

About the vBSIMM

QUESTION:

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

ANSWER:

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: the **vBSIMM (BSIMM for vendors)** and the **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 initiatives via the BSIMM.

QUESTION:

Should the vBSIMM happen in parallel with the BSIMM?

ANSWER:

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 afterward and separately.

QUESTION:

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

ANSWER:

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

ABOUT BSIMM

Started in 2008, the **Building Security In Maturity Model (BSIMM)** is an ongoing 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 variations that make each unique. The BSIMM is not a how-to guide, nor is it a one-size-fits-all prescription. Instead, it is a reflection of actual practices in software security.

Learn more at **bsimm.com**

THE SYNOPSYS DIFFERENCE

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

SYNOPSYS®

185 Berry Street, Suite 6500
San Francisco, CA 94107 USA
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: software-integrity-sales@synopsys.com