Building Security In Maturity Model
(BSIMM)

Bringing science to software security

Change is a constant. Is your SSI keeping up?

- Uptick in development velocity
- Use of automation to drive application lifecycle management processes
- Engineering-led software security efforts
- Shift to containers, microservices, and virtualized environments
- Conflicts in multicloud deployment strategies
- Everything as code
- New application architectures

Overview

Whether software security changes are being driven by engineering team evolution, such as with agile, CI/CD, and DevOps, or originating top-down from a centralized software security group (SSG), maturing your software security initiative (SSI) is critical to your success in managing risk. But what if your team has neither the visibility into the current state of your SSI nor the data they need to create an improvement strategy and prioritize SSI change?

Your solution is to use the Building Security In Maturity Model (BSIMM), a decade-long study of SSIs resulting in a unique industry model and yardstick for measuring SSIs. By quantifying the activities of many different organizations, the BSIMM describes the common ground they share as well as the variations that make each unique. A BSIMM assessment scorecard provides a way to assess the current state of your SSI, identify gaps, prioritize change, and determine how and where to apply resources for immediate improvement.

What the BSIMM enables you to do

1. Start a software security initiative (SSI) using real data.

If you don't have an SSI yet, you need one. As you start down that path, the BSIMM will help you understand the core activities that all successful initiatives undertake—no matter what industry you're in, your company size, your deployment models, or your compliance requirements.

2. Compare your SSI to that of other firms in your industry.

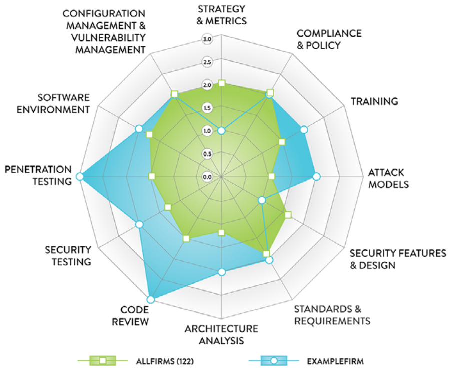
The BSIMM is the only yardstick available today for measuring your SSI and determining how your results compare with other results across multiple industry groups. With your goals in mind, you can quickly determine where you stand relative to your needs.

3. Benchmark and track your SSI growth.

The BSIMM is the best and only repeatable way to measure your SSI's breadth and depth. Once your SSI is established, you can use the BSIMM to measure your continuous improvement year over year. The BSIMM also provides concrete details to show your executive team and board how your security efforts are making a difference.

4. Evolve your SSI using lessons learned from mature initiatives.

The BSIMM is a “what works” report on building and evolving an SSI. It comprises proven activities that mature organizations are performing today. You can use your assessment results, the BSIMM activities, and your objectives to set strategies and priorities for real improvement.



5. Interact with professionals facing common issues.

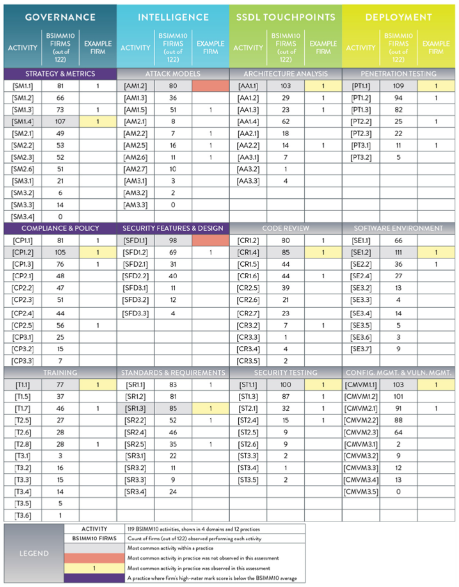
Along with your BSIMM results, you gain access to our exclusive BSIMM community, which includes newsletters, specialized webinars, U.S.- and U.K.- based annual conferences, RSA Conference networking events, and a vibrant online community.

Get a personalized report

Every BSIMM assessment comes with a detailed report highlighting your SSI areas of strength and where it could use improvement. For use with executives and the board, you also get:

Customized Spider Chart. This diagram shows at a glance where you are ahead of the game and where you might be behind. As you switch from measuring-stick mode to SSI-planning mode, these results provide objective feedback so you can track progress.

BSIMM Scorecard. This table shows where you stand relative to other initiatives. You can use it to look at your entire initiative over time, your individual business units, business partners, and the vendors you work with.



GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM10 FIRMS (out of 122)	EXAMPLE FIRM	ACTIVITY	BSIMM10 FIRMS (out of 122)	EXAMPLE FIRM	ACTIVITY	BSIMM10 FIRMS (out of 122)	EXAMPLE FIRM	ACTIVITY	BSIMM10 FIRMS (out of 122)	EXAMPLE FIRM
STRATEGY & METRICS			ATTACK MODELS			ARCHITECTURE ANALYSIS			PENETRATION TESTING		
[SM1.1]	81	1	[AM1.2]	80	🟥	[AA1.1]	103	1	[PT1.1]	109	1
[SM1.2]	66		[AM1.3]	36		[AA1.2]	29	1	[PT1.2]	94	1
[SM1.3]	73	1	[AM1.5]	51	1	[AA1.3]	23	1	[PT1.3]	82	
[SM1.4]	107	1	[AM2.1]	8		[AA1.4]	62		[PT2.2]	25	1
[SM2.1]	49		[AM2.2]	7	1	[AA2.1]	18		[PT2.3]	22	
[SM2.2]	53		[AM2.5]	16	1	[AA2.2]	14	1	[PT3.1]	11	1
[SM2.3]	52		[AM2.6]	11	1	[AA3.1]	7		[PT3.2]	5	
[SM2.6]	51		[AM2.7]	10		[AA3.2]	1				
[SM3.1]	21		[AM3.1]	3		[AA3.3]	4				
[SM3.2]	6		[AM3.2]	2							
[SM3.3]	14		[AM3.3]	0							
[SM3.4]	0										
COMPLIANCE & POLICY			SECURITY FEATURES & DESIGN			CODE REVIEW			SOFTWARE ENVIRONMENT		
[CP1.1]	81	1	[SFD1.1]	98	🟥	[CR1.2]	80	1	[SE1.1]	66	
[CP1.2]	105	1	[SFD1.2]	69	1	[CR1.4]	85	1	[SE1.2]	111	1
[CP1.3]	76	1	[SFD2.1]	31		[CR1.5]	44		[SE2.2]	36	1
[CP2.1]	48		[SFD2.2]	40		[CR1.6]	44	1	[SE2.4]	27	
[CP2.2]	47		[SFD3.1]	11		[CR2.5]	39		[SE3.2]	13	
[CP2.3]	51		[SFD3.2]	12		[CR2.6]	21		[SE3.3]	4	
[CP2.4]	44		[SFD3.3]	4		[CR2.7]	23		[SE3.4]	14	
[CP2.5]	56	1				[CR3.2]	7	1	[SE3.5]	5	
[CP3.1]	25					[CR3.3]	1		[SE3.6]	3	
[CP3.2]	15					[CR3.4]	4		[SE3.7]	9	
[CP3.3]	7					[CR3.5]	2				
TRAINING			STANDARDS & REQUIREMENTS			SECURITY TESTING			CONFIG. MGMT. & VULN. MGMT.		
[T1.1]	77	1	[SR1.1]	83	1	[ST1.1]	100	1	[CMVM1.1]	103	1
[T1.5]	37		[SR1.2]	81		[ST1.3]	87	1	[CMVM1.2]	101	
[T1.7]	46	1	[SR1.3]	85	1	[ST2.1]	32	1	[CMVM2.1]	91	1
[T2.5]	27		[SR2.2]	52	1	[ST2.4]	15	1	[CMVM2.2]	88	
[T2.6]	28		[SR2.4]	46		[ST2.5]	9		[CMVM2.3]	64	
[T2.8]	28	1	[SR2.5]	35	1	[ST2.6]	9		[CMVM3.1]	2	
[T3.1]	3		[SR3.1]	22		[ST3.3]	2		[CMVM3.2]	9	
[T3.2]	16		[SR3.2]	11		[ST3.4]	1		[CMVM3.3]	12	
[T3.3]	15		[SR3.3]	9		[ST3.5]	2		[CMVM3.4]	13	
[T3.4]	14		[SR3.4]	24					[CMVM3.5]	0	
[T3.5]	5										
[T3.6]	1										

LEGEND		
	ACTIVITY	119 BSIMM10 activities, shown in 4 domains and 12 practices
	BSIMM10 FIRMS	Count of firms (out of 122) observed performing each activity
	▨	Most common activity within a practice
	🟥	Most common activity in practice was not observed in this assessment
	1	Most common activity in practice was observed in this assessment
	🟪	A practice where firm's high-water mark score is below the BSIMM10 average

Extracting value

“Since 2008, the BSIMM has served as an effective tool for understanding how organizations of all shapes and sizes, including some of the most advanced security teams in the world, are executing their software security strategies,” said Jim Routh, head of enterprise information risk management at MassMutual. “The current BSIMM data reflect how many organizations are adapting their approaches to address the new dynamics of modern development and deployment practices, such as shorter release cycles, increased use of automation, and software-defined infrastructure.”

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.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com