

BSIMM

Building Security In Maturity Model

Christian.Heinrich@cmlh.id.au



BSIMM explores “What is a Successful Software Security Initiative (SSI) from a Scientific Sample?”

Forked from OpenSAMM Beta i.e. <http://www.opensamm.org/>

Further information is available from <http://www.bsimm2.com/>

BSIMM - Sample Size - USA

Total of **Nine (9)** with **Two (2)** Unnamed out of **25** Most Advanced SSI



Microsoft QUALCOMM

Google EMC²



Financial Services (two (2) declined to be named):
The Depository Trust and Clearing Corporation (DTCC)
Wells Fargo

Independent Software Vendors:
Adobe
Microsoft
Qualcomm

Technology Firms:
Google
EMC

Quoted from p2 or p5 (PDF Page Numbering) of BSIMM v1.5

BSIMM - Sample Size - Europe

Total of **Nine (9)** with **Four (4)** Unnamed out of **56** Most Advanced SSI



The bottom row of logos is two companies i.e. total of five (5).

Financial Services

- Standard Life
- SWIFT

Media and Telecommunications

- Nokia
- Thomson Reuters
- Telecom Italia

Quoted from BSIMM v1.5 p51 or p54 (PDF Page Numbering)

BSIMM2 - Sample Size

Total of 30



Financial Services

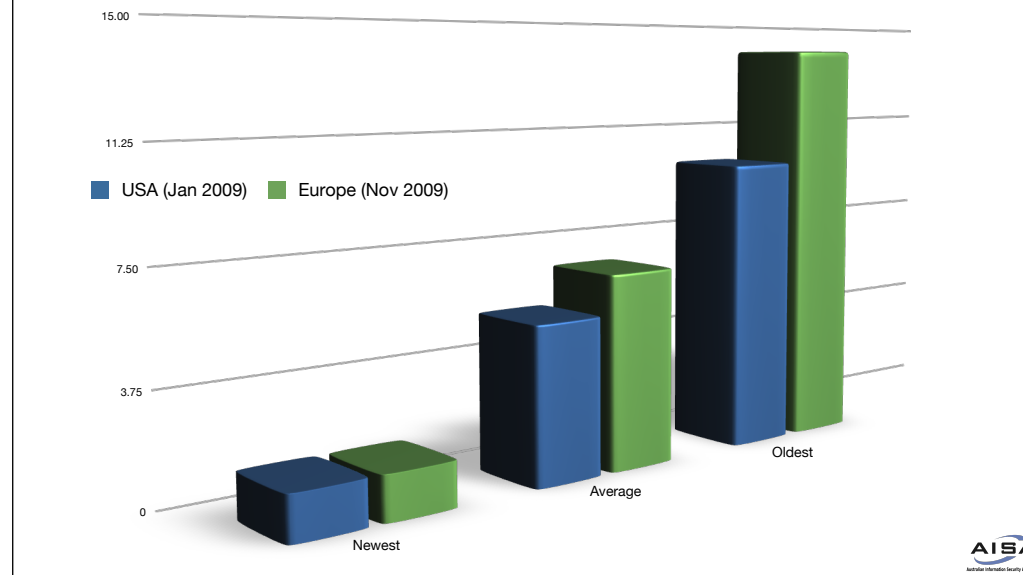
Bank of America
Capital One
SallieMae

Independent Software Vendors

VMWare
Intel
Intuit
Symantec

Quoted from p4 or p7 (PDF Page Numbering) of BSIMM2

BSIMM - SSI Duration - Global



USA - 1 (year) 1/2 (6 months), 5 (years) 1/3 (4 months), 10 (years)

USA Data Quoted from BSIMM v1.5 pp2 and 3 (same as PDF Page Number)

European - 1 1/2 (6 months), 6 2/3 (8 months), 14 (years)

European Data Quoted from BSIMM v1.5 p51 or p54 (PDF Page Numbering)

BSIMM2 - 1/4 (3 months), 4 5/12 (5 Months), 14 Years - September 2009

BSIMM2 is *not* included in the above graph due to similar values with BSIMM (Europe)

Quoted from BSIMM2 p4 or p7 (PDF Page Numbering)

BSIMM - Resourcing - Global

USA - Jan 2009			
	Developer	Satellite	SSG
Median	5000	20	20
Average	7550	79	41
Largest	30000	300	100
Smallest	450	0	12

Europe - Nov 2009			
	Developer	Satellite	SSG
Median	5000	0	11.5
Average	4664	29	16
Largest	12000	140	50
Smallest	400	0	1



Colours used in table signify:

Pink -> Average

Blue -> Less

Purple -> More

Europe has a significant lower number of resources within their SSG compared to the USA. Yet their (European) SSI has been executing for a longer duration.

“Satellite” are professionals outside of the SSG who have an interest in software security” as per the definition quoted from p6 or p9 (PDF Page Numbering) of BSIMM v1.5

BSIMM2 - Resourcing - Global

May 2010			
	<i>Developer</i>	<i>Satellite</i>	<i>SSG</i>
<i>Median</i>	3000	11	13
<i>Average</i>	5061	39.7	21.9
<i>Largest</i>	30000	300	100
<i>Smallest</i>	40	0	0.5

Major variances from BSIMM are highlighted in green
Quoted from BSIMM2 p4 or p7 (PDF Page Numbering)

BSIMM - Top Ten - USA

Ten Core Activities Everybody Does		
	Objective	Activity
[SM1.2]	build support throughout organization	create evangelism role/internal marketing
[CP1.3]	meet regulatory needs or customer demand with a unified approach	create policy
[T1.1]	promote culture of security throughout the organization	provide awareness training
[T2.2]	see yourself in the problem	create/use material specific to company history
[SFD1.1]	create proactive security guidance around security features	build/publish security features (authentication, role management, key management, audit/log, crypto, protocols)
[AA1.3]	build internal capability on security architecture	have SSG lead review efforts
[CR2.1]	drive efficiency/consistency with automation	use automated tools along with manual review
[ST2.1]	use encapsulated attacker perspective	integrate black box security tools into the QA process (including protocol fuzzing)
[PT1.1]	demonstrate that your organization's code needs help too	use external pen testers to find problems
[SE1.2]	provide a solid host/network foundation for software	ensure host/network security basics in place



"3 out of 12 Practices are not implemented i.e.

"Attack Models"

"Standards and Requirements"

"Configuration and Vulnerability Management"

Quoted from BSIMM v1.5 p47/p50 (PDF Page Numbering)

Within the "Governance" Domain:

SM is "Strategy and Metrics" Practice

CP is "Compliance and Policy" Practice

Within the "Intelligence" Domain:

SFP is "Security Features and Design" Practice

Within the "SDL Touchpoints" Domain:

AA is "Architectural Analysis" Practice

CR is "Code Review" Practice

ST is "Security Testing" Practice

Within the "Deployment" Domain:

PT is "Penetration Testing" Practice

SE is "Software Environment" Practice

BSIMM - Top 11 to 13 - USA

Three Core Activities that Most Organizations Do		
	Objective	Activity
[AM1.4]	understand the organization's history	collect and publish attack stories
[SR1.1]	meet demand for security features	create security standards
[CMVM1.2]	use ops data to change dev behavior	identify software bugs found in ops monitoring and feed back to dev

Within the “Intelligence” Domain:

AM is “Attack Models” Practice

SR is “Standards and Requirements” Practice

Within the “Deployment” Domain:

CMVM is “Configuration Management Vulnerability Management” Practice

Table above quoted from BSIMM v1.5 p47/p50 (PDF Page Numbering)

BSIMM - Activities - Global

Governance			Intelligence			SSDL Touchpoints			Deployment		
Activity	US Obs.	EU Obs.	Activity	US Obs.	EU Obs.	Activity	US Obs.	EU Obs.	Activity	US Obs.	EU Obs.
[SM1.1]	4	8	[AM1.1]	5	4	[AA1.1]	5	8	[PT1.1]	9	9
[SM1.2]	8	5	[AM1.2]	6	7	[AA1.2]	4	6	[PT1.2]	2	8
[SM1.3]	6	4	[AM1.3]	2	6	[AA1.3]	8	6	[PT2.1]	3	6
[SM1.4]	7	9	[AM1.4]	7	1	[AA1.4]	3	4	[PT2.2]	2	4
[SM1.5]	7	6	[AM2.1]	3	1	[AA2.1]	4	3	[PT2.3]	1	5
[SM2.1]	7	3	[AM2.2]	6	1	[AA2.2]	2	4	[PT3.1]	2	3
[SM2.2]	4	7	[AM2.3]	5	5	[AA2.3]	5	3	[PT3.2]	2	1
[SM2.3]	7	3	[AM2.4]	5	0	[AA3.1]	2	2			
[SM2.4]	4	8	[AM3.1]	1	0	[AA3.2]	1	1			
[SM3.1]	3	2	[AM3.2]	1	0						
[SM3.2]	1	2									
[CP1.1]	6	7	[SFD1.1]	9	8	[CR1.1]	3	5	[SE1.1]	2	3
[CP1.2]	6	8	[SFD1.2]	6	6	[CR1.2]	7	5	[SE1.2]	9	9
[CP1.3]	9	8	[SFD2.1]	6	4	[CR1.3]	3	0	[SE2.1]	1	3
[CP2.1]	3	3	[SFD2.2]	5	4	[CR2.1]	8	6	[SE2.2]	4	5
[CP2.2]	4	7	[SFD2.3]	4	3	[CR2.2]	5	3	[SE2.3]	2	2
[CP2.3]	5	4	[SFD3.1]	1	1	[CR2.3]	4	2	[SE3.1]	3	6
[CP2.4]	3	4	[SFD3.2]	5	3	[CR2.4]	5	4			
[CP2.5]	5	5				[CR2.5]	5	2			
[CP3.1]	1	1				[CR3.1]	2	2			
[CP3.2]	2	3				[CR3.2]	1	0			
[CP3.3]	2	0				[CR3.3]	1	0			
[T1.1]	9	6	[SR1.1]	5	9	[ST1.1]	5	5	[CMVM1.1]	4	6
[T1.2]	5	1	[SR1.2]	3	2	[ST1.2]	5	0	[CMVM1.2]	6	6
[T1.3]	5	0	[SR1.3]	3	3	[ST2.1]	9	5	[CMVM2.1]	6	4
[T1.4]	7	2	[SR1.4]	4	6	[ST2.2]	2	6	[CMVM2.2]	4	3
[T2.1]	6	5	[SR2.1]	3	5	[ST2.3]	3	1	[CMVM2.3]	2	2
[T2.2]	8	3	[SR2.2]	1	2	[ST3.1]	5	0	[CMVM3.1]	1	0
[T2.3]	1	0	[SR2.3]	4	4	[ST3.2]	7	1	[CMVM3.2]	2	0
[T2.4]	6	5	[SR2.4]	5	4	[ST3.3]	2	0			
[T2.5]	4	2	[SR2.5]	4	6	[ST3.4]	2	0			
[T3.1]	2	1	[SR3.1]	3	2						
[T3.2]	1	1									
[T3.3]	1	2									

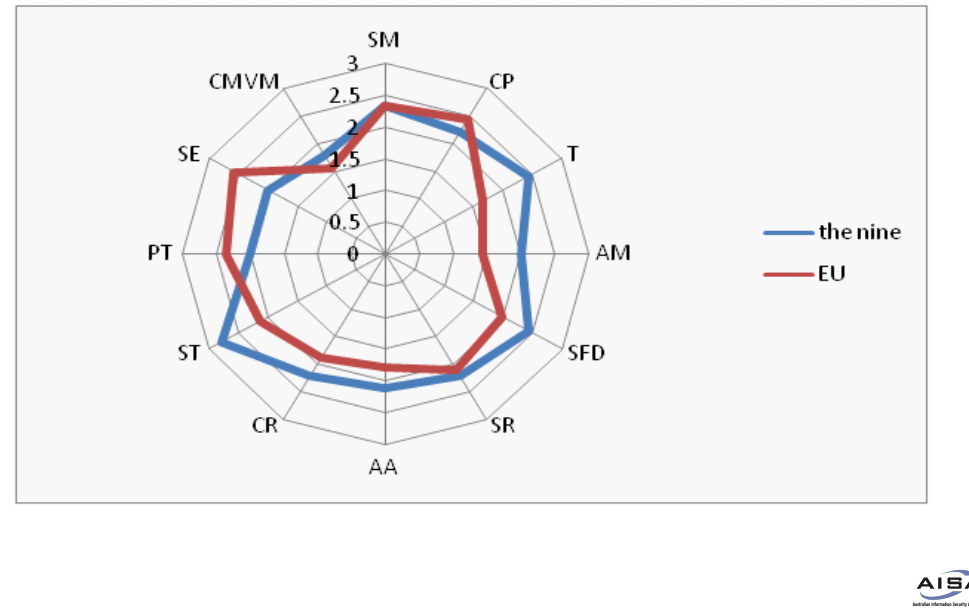


Yellow - 8 out of 9 USA
 Yellow/Blue - More common to USA
 Blue - 8 out of 9 Europe

Table quoted from p53 or p56 (PDF Page Numbering) of BSIMM v1.5

SM is “Strategy and Metrics”
 CP is “Compliance and Policy”
 T is “Training”
 AM is “Attack Models”
 SFD is “Security Features and Design”
 SR is “Standards and Requirements”
 AA is “Architecture Analysis”
 CR is “Code Review”
 ST is “Security Testing”
 PT is “Penetration Testing”
 SE is “Software Environment”
 CMWM is “Configuration Management and Vulnerability Management”

BSIMM - Average - Global



"The largest deltas appear in the Training and Security Testing practices.

There are three practices where the European companies show evidence of more activity: Compliance and Policy, Penetration Testing, and Software Environment.

When it comes to Strategy and Metrics, the averages are exactly the same.

In general, this reflects a European situation that is more process and compliance driven (including privacy compliance) and more driven to measurement.

However, the Europeans tend to carry out fewer assurance activities (for example, reviewing source code to look for bugs) and instead focus more energy getting a handle on the problem and meeting compliance criteria through penetration testing."

Graph quoted from BSIMM v1.5 p52/p55 (PDF Page Numbering)

SM is "Strategy and Metrics"

CP is "Compliance and Policy"

T is "Training"

AM is "Attack Models"

SFD is "Security Features and Design"

SR is "Standards and Requirements"

AA is "Architecture Analysis"

CR is "Code Review"

ST is "Security Testing"

PT is "Penetration Testing"

SE is "Software Environment"

CMWM is "Configuration Management and Vulnerability Management"

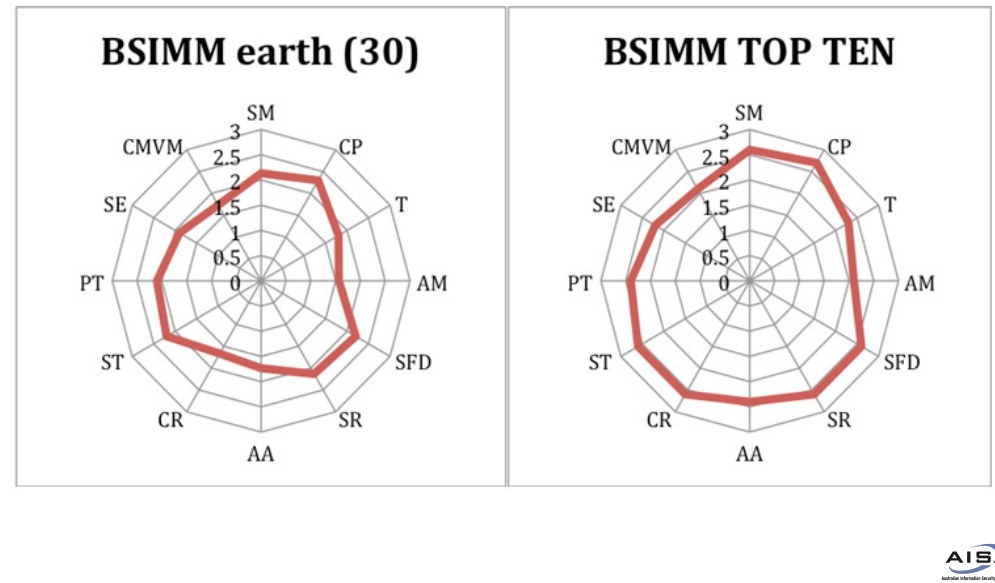
BSIMM2 - Activities

Governance		Intelligence		SSDL Touchpoints		Deployment	
Activity	Observed	Activity	Observed	Activity	Observed	Activity	Observed
(SM1.1)	18	(AM1.1)	12	(AA1.1)	22	(PT1.1)	28
(SM1.2)	18	(AM1.2)	20	(AA1.2)	18	(PT1.2)	17
(SM1.3)	16	(AM1.3)	14	(AA1.3)	19	(PT1.3)	17
(SM1.4)	24	(AM1.4)	10	(AA1.4)	15	(PT1.4)	10
(SM1.5)	13	(AM1.5)	7	(AA1.5)	9	(PT1.5)	11
(SM2.1)	12	(AM2.1)	9	(AA2.1)	6	(PT2.1)	9
(SM2.2)	13	(AM2.2)	13	(AA2.2)	11	(PT2.2)	5
(SM2.3)	16	(AM2.3)	9	(AA2.3)	5		
(SM2.4)	19	(AM2.4)	2	(AA2.4)	3		
(SM3.1)	7	(AM3.1)	2				
(SM3.2)	4						
(CP1.1)	24	(SFD1.1)	29	(CR1.1)	10	(SR1.1)	11
(CP1.2)	24	(SFD1.2)	16	(CR1.2)	19	(SR1.2)	30
(CP1.3)	26	(SFD1.3)	18	(CR1.3)	20	(SR1.3)	16
(CP2.1)	13	(SFD2.1)	11	(CR2.1)	11	(SR2.1)	7
(CP2.2)	18	(SFD2.2)	10	(CR2.2)	8	(SR2.2)	13
(CP2.3)	13	(SFD2.3)	5	(CR2.3)	12	(SR2.3)	6
(CP2.4)	9	(SFD2.4)	10	(CR2.4)	11		
(CP2.5)	17			(CR2.5)	7		
(CP3.1)	4			(CR3.1)	1		
(CP3.2)	7			(CR3.2)	2		
(CP3.3)	5						
(TT1.1)	24	(ST1.1)	22	(ST1.1)	21	(CMW1.1)	21
(TT1.2)	6	(ST1.2)	13	(ST1.2)	9	(CMW1.2)	22
(TT1.3)	5	(ST1.3)	12	(ST1.3)	18	(CMW1.3)	18
(TT2.1)	11	(ST2.1)	11	(ST2.1)	16	(CMW2.1)	11
(TT2.2)	14	(ST2.2)	10	(ST2.2)	5	(CMW2.2)	11
(TT2.3)	13	(ST2.3)	8	(ST2.3)	7	(CMW2.3)	2
(TT2.4)	14	(ST2.4)	13	(ST2.4)	10	(CMW2.4)	4
(TT2.5)	7	(ST2.5)	13	(ST2.5)	3		
(TT3.1)	4	(ST3.1)	11	(ST3.1)	4		
(TT3.2)	3	(ST3.2)	10				
(TT3.3)	4						
(TT3.4)	2						

Fifteen (15) core activities are highlighted in yellow
Quoted from p50 or p53 (PDF Page Numbering) from BSIMM2

SM is “Strategy and Metrics”
CP is “Compliance and Policy”
T is “Training”
AM is “Attack Models”
SFD is “Security Features and Design”
SR is “Standards and Requirements”
AA is “Architecture Analysis”
CR is “Code Review”
ST is “Security Testing”
PT is “Penetration Testing”
SE is “Software Environment”
CMWM is “Configuration Management and Vulnerability Management”

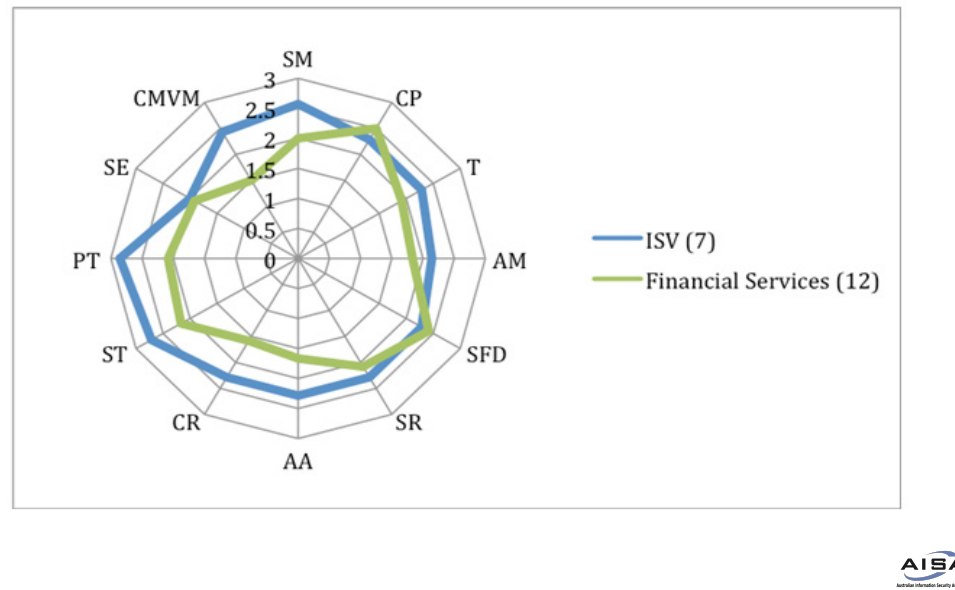
BSIMM2 - Average



Quoted from p9 or p12 (PDF Page Numbering) from BSIMM2

SM is "Strategy and Metrics"
CP is "Compliance and Policy"
T is "Training"
AM is "Attack Models"
SFD is "Security Features and Design"
SR is "Standards and Requirements"
AA is "Architecture Analysis"
CR is "Code Review"
ST is "Security Testing"
PT is "Penetration Testing"
SE is "Software Environment"
CMWM is "Configuration Management and Vulnerability Management"

BSIMM2 - Average



ISV is “Independent Software Vendors” i.e. including Adobe, Microsoft, etc

Quoted from p10 or p13 (PDF Page Numbering) from BSIMM2

SM is “Strategy and Metrics”

CP is “Compliance and Policy”

T is “Training”

AM is “Attack Models”

SFD is “Security Features and Design”

SR is “Standards and Requirements”

AA is “Architecture Analysis”

CR is “Code Review”

ST is “Security Testing”

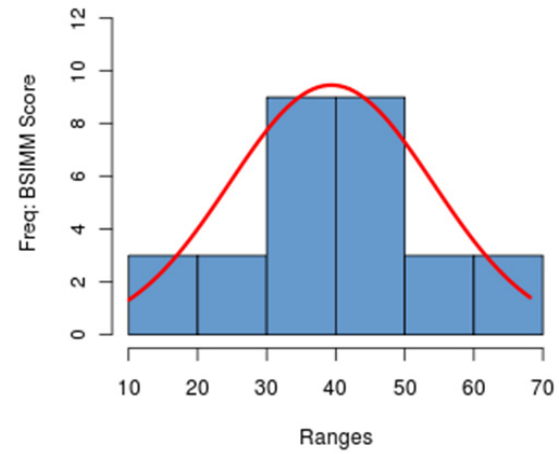
PT is “Penetration Testing”

SE is “Software Environment”

CMVM is “Configuration Management and Vulnerability Management”

BSIMM2 - Average

BSIMM Recursive Mean Score Distribution
Mon Feb 15 16:30:13 2010





Quoted from p10 or p13 (PDF Page Numbering) from BSIMM2

In Closing

Thanks Ricardo, Chris, Audrey and Keith of AISA

Next Presentation at **ISACA**
12PM - 2PM Wed 17 Nov @ Telstra

Slides are published on  slideshare
✦ <http://www.slideshare.net/cmlh>

Slides can be downloaded from 
✦ <http://github.com/cmlh/>