

BSIMM QUESTIONS FOR TEAMS

Welcome, and thanks for taking the time to fill answer the questions below. The objective is to map the existing application security practices to the BSIMM (Building Security In Maturity Model).					<div>PII - Personal Identifiable Information</div> <div>SLA - Service Level Agreements</div> <div>WAF - Web Application Firewall</div> <div>DAST - Dynamic Application Security Testing (BlackBox)</div> <div>SAST - Static Application Security Testing (WhiteBox)</div> <div>N/A - Not Applicable</div>					
Please try to answer the questions bellow quickly, and make a note if you don't understand the question.										
Your name: _____, You role: _____, Team: _____, Today's date: _____										
Application Name: _____, JIRA ID: _____					Version: 0.8 (16/May/2016)					
Type of Application : _____, Technology Stack: _____										
Domain	Practice	Activity	Level	Question	Yes	No	N/A	Maybe	If Yes, 'where is info about it?'	
Governance	Strategy & Metrics	SM1.1		Is there a formal SDL (Software Development Lifecycle) used?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SM1.4		Are there security hooks into the SDL that gather artefacts (new code deployments, test execution results, binaries)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SM2.3		Is there an Security Champion?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	Compliance & Policy	CP1.1		Are there any regulatory or compliance drivers? (to do Security)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		CP1.2		Have PII obligations been identified?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		CP2.1		Does the application holds PII data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		CP2.2		Are compliance-related risks signed off?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		CP2.4		Do 3rd Party vendor contracts have software security SLAs?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		CP2.5		Are executives aware of compliance and privacy obligations?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		CP3.2		Are 3rd parties involved in development?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		CP3.2		Are Security policies imposed on 3rd party vendors?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		CP3.2		Are there security SLAs for 3rd party development teams?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		Training	T1.1		Have all developers received Application Security Awareness training?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	T1.2			Have all developers received role-specific Application Security training?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	T1.6			Is training material specific to current tech stack and company history?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	T1.7			Is there on-demand individual security training?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	T2.5			Do new hires receive Application Security Training?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	T2.6			Do new developers received relevant Security training?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	T3.2			Do 3rd party or outsourced developers receive Application Security Training?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	T3.4			Is there an annual refresh of Application Security Training?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Intelligence	Attack Models	AM1.2		Is there an data classification scheme?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		AM1.2		Is there an inventory of how classified data maps to existing applications?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		AM1.3		Is there a mapping of the attackers to be worried about?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		AM1.4		Is there information on past attacks (successful or not)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	Security Features & Design	SFD1.1		Are there standard security features? (i.e. Secure Controls)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SDF1.2		Are Security Champions (SCs) involved Architecture and Design?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SDF1.2		Are Security Champions doing Threat Models for existing/new Apps or features?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	Standards & Requirements	SR1.1		Are there Security Standards for development?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SR1.2		Is there an Software Security Portal?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SR1.3		Are there Software requirements based on Compliance constraints?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SR2.4		For in-housed developed apps, is Open Source components usage tracked?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SR2.4		For 3rd party dependencies or apps, is Open Source components usage tracked?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SR2.6		Are there Secure Coding Guidelines?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SR2.5		Is there a standard SLA boilerplate for vendor contracts & outsourcing providers? (mapping required Software Security efforts)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		SSDL (Secure SDL)	Architecture Analysis	AA1.1		Have apps been Threat Modelled?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	AA1.4				Is there a risk questionnaire to rank Applications and Features?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Code Review	CR1.1			Is there a list of the most dangerous bugs/vulnerabilities that developers should be aware of?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	CR1.2			Have Security Reviews been done to the released applications?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	CR1.5			Have security-focused code reviews been done on released applications?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	CR2.2			Are secure coding standards enforced?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Security Testing	ST1.1			Does QA perform basic Security or Adversarial tests?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	ST1.3			Are security requirements and security features used to drive tests?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	ST1.3			Are there security focused tests?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	ST2.1			Are there BlackBox (DAST) tools executed by QA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	ST2.3		Is risk analysis used to drive tests?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
	ST2.5		Are there automated security tests executed by QA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
	ST2.6		Are there Fuzz tests executed by QA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
	ST3.4		Is Code Coverage measured for Security tools/tests execution?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
ST3.5		Are there adversarial security tests?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
ation Testing	PT1.1		Have applications been penetration tested?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
	PT1.2		Are penetration tests results added to JIRA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			

Deployment	Penet	PT2.2		Do penetration testers have access to all available information? (for example source-code, JIRA tickets, test accounts)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		PT2.3		Is there an periodic penetration testing sheadule?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Software Environment	SE1.1		Is application live input captured and monitored?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		SE1.1		Is live data sent to InfoSec monitoring systems?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		SE1.1		Is there an WAF protecting the applications?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		SE1.4		Are hosts and networks configured securely?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		SE2.2		Are there secure installation and deployment guidelines?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		SE2.4		Is code developed signed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		SE3.2		Are applications executed with code protection? (DEP, ASLR, VM Sandboxes)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		SE3.3		Are live applications monitored for misbehaviours or signs of attacks?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		Config Management & Vulnerability Mangement	CMVM1.1		Is there an incident response plan?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	CMVM1.2			Are bugs and security issues being identified via live monitoring?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CMVM2.1			Is there an emergency codebase response plan? (i.e. quickly push code fixes to production)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CMVM2.2			Are reported security issues found tracked thought-out its fix process? (reported by code-review, QA, pentest or externally)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CMVM2.3			Is there an operation inventory of deployed applications?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CMVM3.1			Are all reported security issues fixed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CMVM3.2			Is Security SDL changed in order to prevent creating of reported security issues?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Feedback:			Please use this space to enter comments, problems or recommendations (for example missing questions)						

BSIMM QUESTIONS FOR SGS (SOFTWARE SECURITY GROUP)

	Activity	Level	Question	Yes	No	N/A	If Yes, 'where is info about it?' / If No, 'why not?'
Governance	SM1.2		Is there an active SSG (Software Security Group)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SM1.3		Have executives even educated on InfoSec and AppSec?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SM2.1		Is data about software security published internally?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SM2.2		Are there at least two deployment pipelines (with one having the ability to block the release)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SM2.5		Do security metrics exist and published in security portal?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SM2.5		Is Security budget based on real-world metrics and data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SM2.6		Are Security risk explicitly signed off by business owners and management?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CP1.3		Is there an Software Security Policy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CP2.3		Are compliance controls tracked?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CP3.1		Is management security reports and operational data used by compliance assessments?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CP3.3		Does feedback from Secure SDL influence policies?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	T2.5		Are there regular Security Champions meetings? (weekly or monthly)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	T2.7		Is there a process to identify and onboard Security Champions?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	T3.1		Are there rewards (or corporate perks) for Security Champions?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	T3.3		Are there Software Security events hosted internally, but allowing external participation? (for ex: OWASP chapter meeting)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	T3.5		Are there scheduled office hours when Software Security support is provided?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Intelligence	AM1.1		Is there a list of top N possible attacks?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AM1.5		Are new types of attacks and vulnerabilities researched?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AM1.6		Are there collaboration forums for Security Champions? (Slack or mailing lists)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AM2.1		Are attack patterns and abuse cases mapped to attackers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AM2.2		Are technologic specific attack patterns created by internal research teams?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AM3.1		Is there a an internal research team that develops new attack methods?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AM3.2		Is QA able to automate and replicate new types of attacks and exploits?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SFD2.1		Are there secure-by-design frameworks or common libraries?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SDF2.2		Is there capability to support the solution of difficult secure design problems?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SDF3.1		Is there a central group that maintains secure design patterns?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SDF3.2		Is use of approved security features and frameworks required?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SDF3.3		Are mature design patterns documented and published?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SR2.2		Is there a standards review board?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SR2.3		Are there standards for used technology stacks?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SR3.1		Is expose to Open Source vulnerabilities managed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	SR3.2		Are 3rd party vendors aware of existing security standards and policies?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SSDL (Secure SDL)	AA1.2		Are security design reviews performed on high risk applications?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AA2.2		Are architecture descriptions and data flows standardised?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AA2.3		Is Architecture Analysis available as an resource or mentoring?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AA3.1		Does InfoSec or AppSec have software architects that can lead design review efforts?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	AA3.2		Do analysis results feed into standard architecture patterns?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CR1.4		Are static analysis tools (SAST) used to help security code review activities?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CR1.6		Is centralised reporting used to close the knowledge loop and drive training?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CR2.5		Are security tools (when used by developers) supported by mentors?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CR2.6		Are security tools (SAST, DAST) executed with targeted and customised rules?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CR3.2		Are multiple analysis techniques and tools combined into consolidated reports?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CR3.3		Is there the capability to eradicating specific bugs/vulnerabilities from existing codebase?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CR3.4		Is malicious code written by in-house our outsource developers automatically identified?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	ST2.4		Are security results shared with QA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	PT1.3		Are penetration testing tools used internally?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Deployment	PT3.1		Do external penetration testers perform deep-dive analysis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	PT3.2		Are penetration testing testing tools and scripts customised?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CMVM3.3		Are software crisis and attacks simulated?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	CMVM3.4		Is there an bug bounty program?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	