BSIMM QUESTIONS FOR TEAMS

BSIMM Activity	Question	Yes/No	If Yes, 'where is info about it?' / If No, 'why not?'
SM1.1	What is the the SDL (Software Development Lifecycle) currently being used?	☐	
CP1.1	Are the any regulatory or compliance drivers? (to do Security)	☐	
CP2.1	Does the application holds PII data?	☐	
CP3.2	Are 3rd parties involved in development?	☐	
CP3.2	Are there security SLAs for 3rd party development teams?	☐	
T1.1	Have all developers received Application Security Awareness training?	☐	
T1.2	Have all developers received role-specific Application Security training?	☐	
T2.5	Do new hires receive Application Security Training?	☐	
T3.2	Do 3rd party or outsourced developers receive Application Security Training?	☐	
T3.4	Is there an annual refresh of Application Security Training?	☐	
AM1.2	Is there an data classification scheme?	☐	
AM1.2	Is there an inventory of how classified data maps to existing applications?	☐	
AM1.3	Is there a mapping of the attackers to be worried about?	☐	
AM1.4	Is there information on past attacks (successful or not)?	☐	
SFD1.1	Are there standard security features? (i.e. Secure Controls)	☐	
SDF1.2	Are Security Champions (SCs) involved Architecture and Design?	☐	
SDF1.2	Are Security Champions doing Threat Models for existing/new Apps or features?	☐	
SR1.1	Are there Security Standards for development?	☐	
SR1.2	Is there an Software Security Portal?	☐	
SR1.3	Are there Software requirements based on Compliance constraints?	☐	
SR2.4	For in-housed developed apps, is Open Source components usage tracked?	☐	
SR2.4	For 3rd party dependencies or apps, is Open Source components usage tracked?	☐	
SR2.6	Are there Secure Coding Guidelines?	☐	
SR2.5	Is there a standard SLA boilerplate for vendor contracts & outsourcing providers? (mapping required Software Security efforts)	☐	
AA1.1	Have apps been Threat Modelled?	☐	
AA1.4	Is there a risk questionnaire to rank Applications and Features?	☐	
CR1.1	Is there a list of the most dangerous bugs/vulnerabilities that developers should be aware of?	☐	
CR1.2	Have Security Reviews been done to the released applications?	☐	
CR1.5	Have security-focused code reviews been done on released applications?	☐	
CR2.2	Are secure coding standards enforced?	☐	
ST1.1	Does QA perform basic Security or Adversarial tests?	☐	
ST2.1	Are there BlackBox (DAST) tools executed by QA?	☐	
ST2.5	Are there automated security tests executed by QA?	☐	
ST2.6	Are there Fuzz tests executed by QA?	☐	
ST3.4	Is Code Coverage measured for Security tools/tests execution?	☐	
PT1.1	Have applications been penetration tested?	☐	
PT1.2	Are penetration tests results added to JIRA?	☐	
PT2.2	Do penetration testers have access to all available information? (for example source-code, JIRA tickets, test accounts)	☐	
PT2.3	Is there an periodic penetration testing sheadule?	☐	
SE1.1	Is application live input captured and monitored?	☐	
SE1.1	Is live data sent to InfoSec monitoring systems? (Splunk based)	☐	
SE1.1	Is there an WAF protecting the applications?	☐	
SE1.4	Are hosts and networks configured securely?	☐	
SE2.2	Are there secure installation and deployment guidelines?	☐	
SE2.4	Is code developed signed?	☐	
SE3.2	Are applications executed with code protection? (DEP, ASLR, VM Sandboxes)	☐	
SE3.3	Are live applications monitored for misbehaviours or signs of attacks?	☐	
CMVM1.1	Is there an incident response plan?	☐	
CMVM1.2	Are bugs and security issues being identified via live monitoring?	☐	
CMVM2.1	Is there an emergency codebase response plan? (i.e. quickly push code fixes to production)	☐	
CMVM2.3	Is there an operation inventory of deployed applications?	☐	