OWASP SAMM Framework

Megan Leonard

ISEC 475

6/25/2023

OWASP SAMM, software assurance maturity model is a framework that is used for software security based on the risks the organization is against. SAMM is split into 5 different functions that each contain 3 practices totaling 15 different practices. The four different functions are governance, design, implementation, verification, and operations.

Governance creates strategies and training for the model and what policies they need to comply with as they work. The first practice is strategy and metrics, which is where they make an overall plan for the organization’s secure software activities. Then we have policy and compliance where they determine what standards and regulations need to be put into place for this project. The final practice is education and guidance where people are taught about the security software and helps them understand security topics in relation to their job.

Design and Implementation are now two separate functions and were originally combined as construction with the practices: threat assessment, security requirements, and secure architecture. These practices are now under design with the new implementation function containing secure build, secure software, and defect management.

Design looks at the processes and activities that the organization uses to help build the framework. The first practice is threat assessment, which looks at potential threats against the software and the risks to the company. Security requirements look at what is needed for the software to securely complete its tasks. Then security architecture which works on the security of the components that are used in the architecture design.

Implementation focuses on the activities of the organization involving the creation and deployment of the software components. The first practice is secure build which works on making sure that the software is being built to follow standards and can be replicated as needed. Secure deployment follows by checking the security and integrity and making sure they are both intact and ready for deployment. Finally, the defect management that looks at the software security defects and keeps track of them to use as they work on the deployment process.

Verification covers the checks and tests that happen during the software development process. It starts with the practice, architecture assessment which looks over the application and infrastructure to make sure that they are meeting the security requirements and following the policies and compliance requirements. Then we have the requirements-driven testing which makes sure that the controls are operating as intended. Finally, is the security testing with work on testing the different areas of the security to look for bugs or regressions that will need to be fixed.

Operations is the final function and makes sure that the software is able to cover confidentiality, integrity, and availability throughout its time. The first practice is incident management which makes sure that the software can hold against attacks and works on the plan of how to handle vulnerabilities and threats to the system. Environment management helps with keeping it running, implementing any patches it needs and making sure that everything is functioning as it should without problems. The final practice is operational management which looks over the security to make sure it is working as expected during the software lifecycle.

Citation:

*Comparing BSIMM & samm*. OWASP SAMM. (n.d.-a). <https://owaspsamm.org/blog/2020/10/29/comparing-bsimm-and-samm/>

Mead, N. R., & Woody, C. C. (2017). *Cyber Security Engineering: A practical approach for systems and software assurance*. Addison-Wesley.

*The model*. OWASP SAMM. (n.d.-b). <https://owaspsamm.org/model/>

*Owasp Samm*. OWASP SAMM | OWASP Foundation. (n.d.). <https://owasp.org/www-project-samm/>

Pivot Point Security. (2022, June 9). *What is Owasp Samm and why should we (as an org that develops software) care?*. Pivot Point Security. <https://www.pivotpointsecurity.com/what-is-owasp-samm-and-why-should-we-care/>

Software assurance maturity model (SAMM) - owasp foundation. (n.d.). <https://owasp.org/www-pdf-archive/SAMM_Core_V1-5_FINAL.pdf>