**OWASP SAMM Summit 2016 Outcome**

On 20-21 April 2016 our SAMM project team came together in New York to discuss and shape the next releases of OWASP SAMM.

The following topics were covered during our workshops:

* Brief History, Reaffirm scope & mission
* Discuss what to have/keep in the core model as “instruments”?
* Discuss model breadth and applicability
* Review and update the SAMM scoring model towards R1.2
* Discuss the model governance
* Update on the benchmarking initiative
* Detailed discussion on all security practices towards R2.0
* Roadmap towards R2.0

Notes were taken during the workshops and are available here:

<https://docs.google.com/document/d/15MvMU7MXyTpI4GeJmPGaMZnH3eaIq1DtUlp1V7ybvIQ/edit>

**Updated OWASP SAMM Mission (proposal)**

The mission of OWASP SAMM is to be the prime maturity model for software assurance that provides an effective and measurable way for all types of organizations to analyse and improve their software security posture. OWASP SAMM supports the complete software lifecycle, including development and acquisition, and is technology and process agnostic. It is intentionally built to be evolutive and risk-driven in nature.

Key principles include:

* measurable: the framework provides well-defined and discrete levels to support an effective reasoning on software assurance activities ;
* risk-driven: the model is built around risk to optimize the return-on-investment for security spending ;
* full lifecycle: “software supply chain - the model serves both software development and software acquisition” ;
* process and company independent: the model works for different development models, including waterfall and agile, and wants to serve all types of organizations (large versus small, governmental versus commercial, etc.) ;
* evolutive: the approach embraces evolution and is designed to support changes in your organisation, in software development practices (e.g., waterfall versus agile), and in technology (e.g., local versus cloud setups, saas).
* Open: “to be completed”

\* texts between “” to be updated.

**Updated roadmap:**

**Next 1.2 release, updated scoring:**

* Recover source and move it to an asciidoctor based document.
* Clarification of maturity levels (syntactic changes to keep the text consistent)
* Not change activities but try to impose the current scoring system on existing activities, i.e. move from binary yes/no to the multi-tiered questions/answers of the current proposal.
* Show improvements with every activity introduced
* Adapt for the new scoring method
* Update questions for 4-tiers
* Review and where necessary clarify current questions
* Consider v1.1 remarks that were not withheld for the previous release
* **Targeted completion date:** end of september in time for Appsec USA (October 11, 2016)

**SAMM version 2.0**

* Core model changed
* Visualisations + flavours for a few development methodologies
* Update quickstart guide, TB, HTG.
* Success metrics: How well does the model work: Linked to the benchmarking project.
* **Timing**: Target release appseceu 2017. Target rc release for samm summit 2017