Review and suggestions on document “OpenSAMM Quick Start Guide” version of Dec 10th 2014 (in reference to email: http://lists.owasp.org/pipermail/samm/2014-December/000609.html)

1) There are various references to the framework in the quick start document: OpenSAMM, SAMM, Open SAMM, etc.
   I suggest choosing one and only one way to refer to the framework and stick to it across the entire document. For example: OpenSAMM.

2) [Introduction]
   I kind of disagree with the statement “OpenSAMM helps organizations understand […] their SDLC”. According to the source document, it was designed to help organizations formulate and implement a software security strategy that can be fully integrated into their existing SDLC. The original description seems to better match what OpenSAMM does.

   I suggest replacing with:
   “**OpenSAMM is an open framework designed to help organizations formulate and implement a software security program that can be easily integrated into their existing SDLC.**”

3) [Introduction]
   “Like any new framework, it can be difficult…is to try it out.” → this is a negative statement, and I fail to identify the need to start the document this way. First, it brings bad light on frameworks in general ☺. Second, it generalizes their level of difficulty: which would probably be wrong. Third, if someone is reading the quick start guide, I fail to see the logic behind recommending the reader to “try it out”. This text should actually be located somewhere that recommends the reader to download and read the quick start guide, rather than in the quick start guide itself.

   I suggest simply completely removing this statement. Optionally replacing it with:
   “This quick start guide will guide you into setting up an OpenSAMM-based software security program tailored to your organization’s existing software development lifecycle, and rapidly achieve the OpenSAMM Level 1 maturity level within the next weeks or months, depending on your objectives.”

4) [From “SAMM provides” (page1) to “fit your organization and its needs” (page 3)]
   This looks like a summary about OpenSAMM rather than a quick start guide. I would expect a quick start guide to give me initial raw actions that would enable me to quickly start “using” or “adopting” a larger and more complex concept. Of course these steps should not jeopardize a future wider adoption of the framework.

   I suggest removing all of it.

5) [Start your journey] This seems to be the actual quick start guide.
   Each bullet below will cover specific steps inside the list of actions.

6) [Step 1]
   I don’t see the value in telling the reader to go read the full documentation as a first step

when the actual goal of the quick start guide is to simply start…quickly.

Suggestion: remove it from the quick start guide. Maybe transfer it into the future OpenSAMM 1.1? -> having a link to a quick start guide in the introduction might be a good point.

7) [Step 2]
OpenSAMM defines 2 categories of assessments: lightweight and detailed. The lightweight does not require “verifying/auditing” the answers, which would be a good candidate for a quick start. Either this is explicitly specified, or the proposed resource/tool implicitly covers that distinction (see next paragraph).

Too many tools are listed. The 3rd resource seems to be the only one that brings the necessary value: there is no need to read the OpenSAMM document to answer the questions, and the 2nd tab contains guidance to quickly provide the information needed and to translate the answers into OpenSAMM maturity levels.

I recommend removing resources 1 and 2 to simplify this step.

The “Purpose” cell suggests this actions aims at “seeing if you have all the proper processes and tools in place”, which would obviously never be the case. I suggest replacing the “Purpose” with: “Identify the level of maturity of your organization in each of the 12 OpenSAMM software security activities” ← this both describes the step as-is and implicitly delivers educational clues (Maturity Levels, 12 activities, etc.) to the reader.

8) [Steps 3 and 4]
Completing steps 3 and 4 as they are defined actually requires a full understanding of how OpenSAMM works, its processes and concepts and also results in a somewhat full implementation of the framework process right from the quick start guide. To my understanding, this would defeat the concept of a “quick start guide” (maybe consider merging this into the “OpenSAMM cheatsheet” document that Bart proposed, this would be fully adequate).

I saw 3 types of orgs that may be starting an OpenSAMM-based program. I would suggest we consider these three scenarios (at least) after an organization has completed the lightweight assessment:
- Scenario 1 “Level 0 organizations” : Organizations starting from ground zero ← those are the ones who really need our help in getting rapidly into OpenSAMM without getting scared before they even start.
- Scenario 2 “Intermediate organizations”: Organizations that perform appsec without any strategy/governance ← those will probably have reached maturity levels 0+ or 1 in several activities, probably not all of them.
- Scenario 3 “Mature organizations”: Organizations that already perform appsec with strategy/governance and probably follow another framework or standard ← those would probably check many requirements in the maturity levels 2/3 but will probably lack lots of small pointy tasks that are still required to achieve maturity levels 0 and 1 (such as organizations that don’t document stuff or simply buy COTS scanners without understanding what they actually do).

At this point, the quick start guide needs to either:
- Identify a specific audience and deliver a specific quick start guide for that audience
- Adopt a "one-fits-all" strategy, which would result in audience-specific recommendations.
This would typically look like a "Step 5" with 3 different sections (Level-0 orgs, Intermediate orgs, Mature orgs) and specific instructions:
- Level-0 orgs: objective is to reach OpenSAMM Level 1
- Intermediate orgs: objective is to identify a target and define a roadmap to reach it
- Mature orgs: objective is to identify the missing gaps to achieve OpenSAMM Level 3

→ do we agree that this should be answered?
→ was this question already answered? (I couldn't find it in the meeting logs)
→ it this open for discussion? (maybe at a next meeting?)

9) [Step 5]
"Implement the plan and return to step 2"
If you implement the plan, there is no need to conduct a self-assessment right after it because you know you implemented it. Additionally, those are two very distinct activities that should be kept separated in the guide. "Implement the plan" relates to the "Do", whereas the "Return to step 2" relates to the "Check" steps of the PLAN/DO/CHECK/ACT logic.

Suggestion:
- split step 5 into steps 5 and 6
- Content of step 5 may need to be reformulated, depending on conclusions reached after processing bullet #7 above.
- Step 6: "Return to step 2" -> this step aims at initiating the continuous process improvement/feedback loop that is required by most ISO standardized processes.

Kind regards,

Antonio