Objective is to review the SM practice and create a list of improvements.

Current texts:
https://www.owasp.org/index.php/SAMM_-_Strategy_&_Metrics_-_1
https://www.owasp.org/index.php/SAMM_-_Strategy_&_Metrics_-_2
https://www.owasp.org/index.php/SAMM_-_Strategy_&_Metrics_-_3
Or download the latest PDF:
https://github.com/OWASP/samm/blob/master/v1.1/Final/SAMM_Core_V1-1-Final-1page.pdf

The notes below are from the NY Summit:

- Page 19: SM1
    - The governance business should be aligned with the OWASP CISO guide (part of better integration with OWASP)
    - Activity A: Consider making it about building a business case for an assurance programme.
    - Should the necessity to build a maturity programme be at level 1 or 2?
- SM2:
    - Mention the need for a software security group
- SM3:
    - 3A is completely unrealistic. Consider making it an extra activity (i.e. 3+)
    - No decision on whether to move Collecting metrics for historic spending to 3+.
- SM (general):
    - There is currently no mention of executive buy-in in SM.
    - No mention of acting on metrics.

Risk-based model: Which activities should be performed by which types of organizations. Bsimm mainly gives a list of activities without further explanations.
What's appropriate for an organisation?
Currently in the SM activity but hidden. Needs to be expanded and made more visible.

Model does not support risk-based categorisation sufficiently deeply. It is mentioned in the SM and nowhere else. Yes a number of activities are described in terms of high-risk applications.
Model should refer back to risk classification sufficiently frequently to enforce its importance.

All notes from the summit:
https://docs.google.com/document/d/15MvMU7MXyTpI4GeJmPGaMZnH3eaIq1DtUlp1V7ybvIQ/edit

Guidance on how to review & improve the practice:

1. Review the objective: do we change it or do we keep it the same?
2. Activities: What is good and what do we want to keep from the current practice & activities?
3. Levels: are the activities grouped in the right levels, or do we need to change levels?
4. Are there activities to drop?
5. Are there activities to add?

Some general principles to keep in mind:

- Should we make distinction between developed software and acquired software? No. same activities should be performed. How they are accomplished (within the model) might differ.
- Keep it process-independent:
  - Should focus more on compatibility with devops movement (without losing the gains security has made during non-devops sdlc).
  - Address cloud environment where organisations don't own the infrastructure they deploy on
- It's a maturity model designed to measure a company's maturity level.
- Model should clarify a story, why should various activities be done, how do they fit together (aka guidance on a process roadmap).

Review practice applicability:

- How well does the model apply to different types of organizations?
  - Government
  - Enterprise
  - Small business
  - Start-up / Scale-up
- How should the model handle the differences?
  - Across bigger portfolios
  - Expert dependencies

Review practice breadth:

- Does the practice accurately portray the current landscape of software assurance?
  - Dev Methodologies (Waterfall, Agile, DevOps)
  - Software Components (built, OSS, outsourced, "software supply chain", etc.)
  - Deployment Infrastructure (On-Premises, Cloud, Mobile, Hybrid, etc.)
  - Compliance (Audit, Legal, Privacy by Design, etc.)
- Do we think it will change in the coming 2-5 years?
- What assumptions does the current model make that need to be revised/removed?
- Dependencies on IT maturity (and others) outside of "security" represented?

Add your improvement suggestions below (you can already do this prior to the call):

Placeholder (copy/paste)
Improvement #: 1
Practice / Level / Activity: Lay the land of past/recent security incidents
Improvement:
Suggested text:
Rationale:

Call 28-Sep-2016
Present:

- Seba
- Bruce Jenkins
- David Schneider

- Daniel walden
- Bart
- Hardik
- …

Input from Daniel Kefer per email:
1) I was thinking a lot about scope of SAMM especially when it comes to acquiring SW. I know that we want to be universal, but where do we end? with e.g. scenarios like buying workstations with client sw, network printer, IoT... These are usually not a part of an appsec programm from what I've seen so far...
2) in the first level, one of the important things I see actually defining an owner of the topic with focus on scalability on higher levels.
3) not sure about how much I'd focus on long term planning/roadmaps nowadays, I think it's more about fast adaptation and alignment with business.
4) I like that metrics comes rather in higher levels, that's what I see in most organizations as well.

Notes from the call:

Level 1:

- Need to add “creating business case” + or even before: assessment if this makes sense
- “Lay out the land” to get attention & executive support - # data breaches … = doing awareness - link your threats to “your environment” - tie incidents to your organisation
- Scoping part of roadmap ?
- Does it make sense to

Step back to look at basic meanings of the levels.
Keep in mind that the levels will be redefined.
We might have level “3+” activities

We do not see a lot of orgs that do Lev3actA?

Current Lev1ActA :

+ make external references explicit + look at environment.
+ Consider moving (parts of this) to TA practice?
+ Include parts in the business case

Cfr ISO27K1 methodology or Octave = risk analysis

Current Lev1ActB:

+ Consider splitting assessment (Lev 1) + creating roadmap (Level 2)
+ Scope discussed?
+ “Chicken & egg” situation

Add activitity: create the business case / get mgmt buy-in / get budget (Level 1)
=> critical to start the program

Lot of orgs do “ad-hoc” activities without a roadmap. A roadmap is more efficient (ie level 2)

Do proof of concepts on part of the org and then based on LL roll it out towards rest of org.

Creating a “draft” instead of a “5-year” program. Going for a more “agile & iterative” development. Start with the draft and then improve in followup iterations.

Level 2
Act A - very important + keep at this level
Focus on applications AND data
Data classification is known by most organisation, application classification is “new”. This can take into account data classification as one of the parameters, together with others such as Internet facing or not , …
IMPORTANT activity: to be stressed and integrated more into the model

How about swapping L1B with L2A: makes sense!!!

L2B - keep as is + ties into “gate” L3 activities of Verification practices

L3A - not done overall - need this as part of maturity model?

= not in span of control
Alternative: Tie spend to levels - putting budget on high risk applications - review this

What is missing: nowhere do we mention the effectiveness of the program (L2), to be done before optimizing. (L3)

Adding metrics / dashboard of #detected & #fixed vulnerabilities for application portfolio?
How to measure impact of activities.

L3B - difficult to measure (its everyone's job …),

Action: create a draft outline for the next meeting (to discuss for 15 minutes - Hardik volunteers

- + Then we schedule Policy&Compliance

By 4th Wed of October.