# SAMM – Conducting Assessments Notes

To what level of detail are people going into with their assessments and how can we tailor SAMM to the most common assessment types.

Point made – Assessment criteria

* Ask questions that reside within the model
* Questions can be misconstrued
* Open ended questions
* End Users tend to overestimate whilst management under sell, important to spread questions across hierarchy
* Getting rid of self-assessment is not viable for majority of companies
* Split self-assessment into two or three roles, coding questions to developers etc.
* Self-assessment allows for people to gain more understanding with their programme
* How do you quantify answers?
* Give priority of answer to the person that should have most knowledge if there is a disagreement
* More in-depth code review
* How do you cover fluid development processes?
* Focus on a standardised setup
* Assessment type agnostic
* Consider aligning maturity levels to adopted standards (research CMMI?)
* A metric based approach involves many variables such as framework, balancing, incentive etc.
* Fast and inexpensive
* Assessment conclusions should make sure that applications aren’t moving in the wrong direction regarding security
* Changes can’t be hugely drastic

‘

Key Takeaways

Team questionnaires

CMMI research