# SAMM Sessions – Core Model Update 2 – Dev Methods

Look at security practices in the core model and see how to apply restructuring to the key practices. Regrouped or restricted to better reach the objectives.

Six activities aren’t overtly clear so it’s important to clarify further.

Develop design principals to give to teams to work from.

Can an objective be achieved without completing activities, how do we plan for this situation?

Less activities but fewer with more depth.

Want to support as many methodologies as possible (agile, waterfall etc.), this makes it important that activities are applicable to all different types and it doesn’t penalise/not apply to development processes that don’t fit under revised activities.

The current model is very inconsistent.

**Security architecture**

Two objectives are needed – Design support and Dependency management. With these objectives tailoring the two primary activities to each different objective.

How well are the objectives/activates being implemented, whilst there is quantitative date, qualitative is missing.

How do we apply design patterns?

Simplify activities, more consistent and understandable. Activities must apply to any lifecycle.

Clearly define what the maturity levels mean to make the benefits clear to DevOps.

The maturity levels must lead into one another rather than assuming people will go through the levels sequentially.

Two are a core model level symmetry etc. Or if there is room for more activities they could added to an “extended model”. This allows for people to continue securing their applications.

**Implementation review**

Can you get to IR3 doing completely automated or manual reviews?

Two threads one is for automated review processes and the other is for manual processes. In order to achieve level 3 you will need to have completed both threads. This creates a more comprehensive review, manual can find things tools cannot, whilst automated allows for a wider scale.

Manual Thread

Level 1- A set of basic guidelines with someone that can do a review of high risk code

Level 2 – Standardise rules that are being used for a review. An independent party should be used for the review.

Level 3 – The lessons learned from the previous levels should stamp out some of the earlier issues, if issues have not decreased it may come down to education etc.

Automated Thread

**Key Takeaways**

We restructure the SAMM activities with increasing maturity of implementation.

We will apply this overall on all the SAMM practices/activities (high level)

We will create one or more detailed descriptions with implementation guidance