Introduce OWASP SAMM – to attain software assurance maturity:

- The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. SAMM helps you:
  - Evaluate an organization's existing software security practices
  - Build a balanced software security assurance program in well-defined iterations
  - Demonstrate concrete improvements to a security assurance program
  - Define and measure security-related activities throughout an organization
- SAMM provides a model for organisations to assess their current level softwar capabilities. It is not expected nor is it required that an organisation should achieve the maximum maturity level in each category. Instead organisations are encouraged to determine the target maturity levels for each Security Practice that best fits the organisation's goals, and adapt the SAMM templates accordingly.
- Structurally SAMM defines five critical business functions: ¬
  - Governance
  - Design
  - Implementation
  - Verification
  - Operations
- Each business function has three security practic itself, which can be described through three levels of maturity: Level 0: an implicit starting point with an unfulfilled Security Practice ¬
  - Level 1: an initial understanding and ad hoc
  - Level 2: a structured realisation with increased efficiency and effectiveness of the Security Practice
  - Level 3: a comprehensive mastery of the Security Practice at the scale that comes with an optimised solution.
- For each level, SAMM defines the objective, a set of activities and describes expected results.
- How is SAMM utilised in practice? With just four (more or less) easy steps:

  1. Assess the organisation's current software security posture
  2. Define the organisation's targets for each Security Practice
  3. Define the implementation roadmap to achieve the set targets
  4. Make it so! Do the necessary work to implement it all.