# How to Conduct an OWASP SAMM Self-Assessment

Maturity assessment, scoring, and improvement roadmaps

## Step 1: Understand the SAMM Model

OWASP SAMM (Software Assurance Maturity Model) measures security practices across 5 business functions, each with 3 practices:

- Governance: Strategy & Metrics, Policy & Compliance, Education & Guidance
- Design: Threat Assessment, Security Requirements, Security Architecture
- Implementation: Secure Build, Secure Deployment, Defect Management
- Verification: Architecture Assessment, Requirements Testing, Security Testing
- Operations: Incident Management, Environment Management, Operational Management

Each practice has 3 maturity levels (1-3). Level 0 means no structured activity.

## Step 2: Run the Assessment

Gather a cross-functional team and score each practice:

- Schedule 2-4 hours with representatives from dev, security, ops, and management
- For each practice, review the SAMM activity descriptions and evidence criteria
- Score honestly: partial implementation = lower level (don't round up)
- Document evidence for each score (tools in use, policies, training records)

## Step 3: Build Improvement Roadmap

Use the gap analysis to prioritize improvements:

- Define target maturity levels per practice (not everything needs to be level 3)
- Prioritize: high business impact + low current maturity = highest priority
- Create 90-day improvement sprints with specific, measurable goals
- Reassess every 6-12 months to track progress and adjust targets