

8 SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SSDLC): ANALISI DELLE METODOLOGIE E DEI PROCESSI

8.1 Life Cycle & Maturity Models

8.1.1 Software Assurance Maturity Model (SAMML)

SAMM è un framework aperto per aiutare le organizzazioni a formulare e attuare una strategia di sicurezza software, che più si adatti ai rischi specifici della particolare organizzazione. Il progetto OpenSAMM, un'attività di OWASP, mantiene e aggiorna la documentazione SAMM.

References	www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model www.opensamm.org www.opensamm.org OpenSAMM
-------------------	---

Le risorse fornite da SAMM attraverso il sito web aiutano a:

- Valutare le pratiche di sicurezza software esistenti di un'organizzazione
- Costruire un programma software security assurance in iterazioni ben definite
- Dimostrare miglioramenti concreti al programma di security assurance
- Definire e misurare le attività relative alla sicurezza in tutta l'organizzazione

Essendo un progetto Open, i contenuti SAMM sono liberamente fruibili. Il modello si basa su 4 funzioni aziendali (Governance, Construction, Verification e Deployment) di sviluppo software e di 12 procedure di sicurezza. Ogni funzione all'interno dello sviluppo del software prevede tre pratiche di sicurezza:

- Governance
 - Strategy & Metrics
 - Education & Guidance
 - Policy & Compliance
- Construction
 - Security Requirements
 - Threat Assessment
 - Secure Architecture
- Verification
 - Design Review
 - Security Testing
 - Code Review
- Deployment
 - Environment Hardening
 - Vulnerability Management
 - Operational Enablement