

The Software Security Framework (SSF)			
Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

Figura 15 - BSIMM SSF

Per ogni livello di pratica e di maturità vi è un'associazione "one activity - one objective". I domini sono:

1. Governance - Pratiche che aiutano a organizzare, gestire e calibrare un framework di sicurezza del software. Anche l'addestramento del personale è una pratica da far rientrare nella governance centrale.
2. Intelligence - Un insieme di conoscenze aziendali utili per svolgere attività di sicurezza del software all'interno di un'organizzazione; comprende sia indicazioni proattive sulla sicurezza che modelli di organizzazione delle minacce.
3. SSDL Touchpoints - Pratiche associate all'analisi e alla sicurezza di particolari sviluppi software, artefatti e processi. Tutte le metodologie di sicurezza del software includono queste pratiche.
4. Deployment - Pratiche che si rifanno alla sicurezza della rete tradizionale e alla manutenzione del software. La configurazione del software, la manutenzione e altri problemi ambientali hanno un impatto diretto sulla sicurezza.

Il modello di maturità si presenta come una serie di attività connesse con le pratiche. Gli obiettivi per ogni livello di pratica sono identificati. Gli obiettivi possono essere ulteriormente suddivisi in obiettivi per la pratica/livello e sono associati alle attività. A titolo di esempio, la figura seguente, tratta dal documento BSIMM2, mostra il modello di maturità per la pratica di addestramento del dominio Governance.