In accordo al (ISC)², il CSSLP è progettato per:

- Stabilire le migliori pratiche, al fine di limitare la proliferazione delle vulnerabilità di sicurezza che derivano da processi di sviluppo insufficienti
- attestare la capacità professionista di mitigare i problemi di sicurezza e dei rischi che circondano lo sviluppo di applicazioni in tutto il SDLC, dalla specifica e progettazione alla realizzazione e manutenzione

I seguenti domini compongono il CSSLP Common Body of Knowledge (CBK), che si concentra sulla necessità di integrare la sicurezza nel SDLC:

- Secure Software Concepts: implicazioni di sicurezza nello sviluppo di software.
- Secure Software Requirements: catturare i requisiti di sicurezza nei raccolta dei requisiti di fase
- Secure Software Design: tradurre i requisiti di sicurezza in elementi di design di applicazioni
- Secure Software Implementation/Coding: unit testing per la funzionalità sicurezza e la resilienza contro gli attacchi, e lo sviluppo di codice sicuro e sfruttare la mitigazione
- Secure Software Testing: test integrati di quality assurance per la funzionalità sicurezza e la resilienza contro gli attacchi
- Software Acceptance: implicazioni per la sicurezza in fase di accettazione del software
- Software Deployment, Operations, Maintenance and Disposal: problemi di sicurezza intorno operazioni di steady-state e la gestione del software.

La qualificazione CSSLP è valida per tre anni, dopo di che deve essere rinnovata. Può essere rinnovata rifacendo l'esame o, più comune, con l'acquisizione di crediti formativi professionali (CPE).

Il CISSP, un altro programma di certificazione da (ISC)² con regole simili, è destinato ai professionisti che sviluppano politiche e procedure in materia di sicurezza delle informazioni.

7.7 Certificazioni ISACA (CISA, CISM, CRISC)

Le certificazioni ISACA sono accettate e riconosciute a livello globale e sono destinate al management IT per rafforzare le loro competenze negli ambiti: audit IT, sicurezza, governance e gestione dei rischi. Nel dettaglio:

- Certified Information Systems Auditor (CISA). Certifica le competenze necessarie ad amministrare e controllare l'IT dell'azienda e a compiere un effettivo audit sulla sicurezza dell'organizzazione. La certificazione CISA ha per oggetto le seguenti aree: Processo di audit dei sistemi informatici; IT Governance e Management; Acquisizione, sviluppo e implementazione dei sistemi informatici; Operazioni, mantenimento e supporto dei servizi informatici; Protezione delle risorse informatiche.
- Certified in Risk and Information Systems Control (CRISC), prepara e abilita i professionisti IT alle sfide IT e alla gestione dei rischi aziendali. La certificazione CRISC ha per oggetto le seguenti aree della gestione degli IT Risk: Identificazione, e Valutazione dei Rischi; Risposta ai Rischi; Monitoraggio dei rischi; Impostazione e implementazione dei controlli IT; Monitoraggio e manutenzione dei controlli IT.
- Certified Information Security Manager (CISM). La certificazione CISM ha per oggetto le seguenti aree: Governance della sicurezza delle informazioni; Gestione dei rischi e Conformità; Sviluppo e Gestione dei programmi di Sicurezza delle Informazioni; Capacità di reagire agli incidenti di sicurezza.