CSSLP[CM]

SOFTWARE PROFESSIONALS

Take the Lead in Securing Software in the SDLC

The Certified Secure Software Lifecycle Professional (CSSLP[CM]) is the only certification in the industry designed to ensure that security is considered throughout the entire software lifecycle. From concept and planning through operations and maintenance to the ultimate disposal, it establishes industry standards and best practices for building security into each phase.

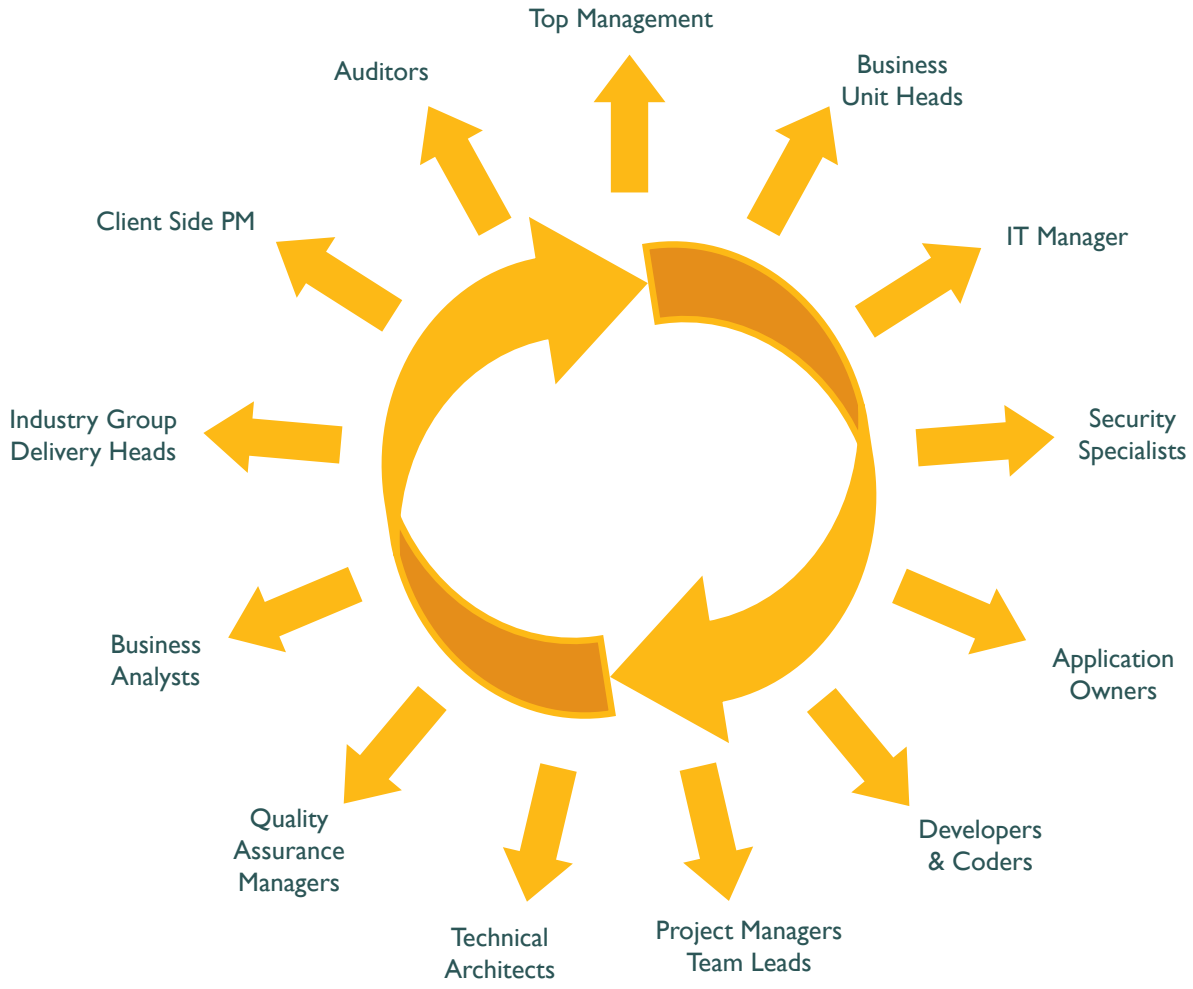
Confidentiality, integrity, availability, authentication, authorization and auditing – the core tenets of security – must become requirements in the software lifecycle. Without this level of commitment, information is placed at risk. Incorporating security early and maintaining it throughout all the different phases of the software lifecycle has proven to be 30-100 times less expensive and incalculably more effective than the release and patch methodology used frequently today.

CSSLP demonstrates competence in the seven domains of the (ISC)[2]® CSSLP CBK® and acknowledges the years of experience attained. These seven domains are explained in the (ISC)[2] CSSLP CBK Education Program brochure, and are as follows:

- **Secure Software Concepts –** security implications in software development and for software supply chain integrity
- **Secure Software Requirements –** capturing security requirements in the requirements gathering phase
- **Secure Software Design –** translating security requirements into application design elements
- **Secure Software Implementation/Coding –** unit testing for security functionality and resiliency to attack, and developing secure code and exploit mitigation
- **Secure Software Testing –** testing for security functionality and resiliency to attack
- **Software Acceptance –** security implication in the software acceptance phase
- **Software Deployment, Operations, Maintenance and Disposal –** security issues around steady state operations and management of software

CSSLP[CM]

CSSLP[CM] is for all software lifecycle stakeholders with at least four years professional experience.



Roles a CSSLP plays within his/her organization:

- Provides a holistic approach to software security needs
- Gives advice regarding designing, developing and deploying secure software
- Maintains knowledge on the latest software security technologies
- Assists in meeting the assurance of compliance to regulations
- Affirms compliance to the policy & procedures set

You're a Critical Stakeholder - Don't Overlook Building in Security.

Here are some vital reasons that security MUST be considered in the SDLC*:

- **May 2009 –** 65,000 of Aetna's current and former employees **Social Security Numbers** may have been **compromised** in a Website **data breach.**
- **Jan 2009 –** With 100 million transactions per month, Heartland Payment Services found evidence of **malicious software** that compromised card data across their network. This incident may be the result of a global cyberfraud operation.
- **Dec 2008 –** 1.1 million Social Security **records exposed** when **hackers** broke into RBS WorldPay's systems.

Any stakeholder who is responsible for creating software must devise ways to ensure applications are built securely. The following best practices will help to ensure that the software released is less susceptible to security breaches.

The Ten Best Practices

1. Protect the Brand Your Customers Trust
2. Know Your Business and Support it with Secure Solutions
3. Understand the Technology of the Software
4. Ensure Compliance to Governance, Regulations, and Privacy
5. Know the Basic Tenets of Software Security
6. Ensure the Protection of Sensitive Information
7. Design Software with Secure Features
8. Develop Software with Secure Features
9. Deploy Software with Secure Features
10. Educate Yourself and Others on How to Build Secure Software

Check out other whitepapers at: **www.isc2.org/csslp-whitepapers**

*Data taken from US - Chronology of Data Breaches

CSSLP[CM] candidates must meet the following requirements prior to taking the CSSLP examination:

- Have a minimum of four years of direct full-time work experience in the SDLC process or three years of direct full-time work experience in the SDLC process with a college degree.
- Complete the Candidate Agreement, attesting to the truth of his or her assertions regarding professional experience and legally commit to adhere to the (ISC)[2®] Code of Ethics.
- Successfully answer four questions regarding criminal history and related background.

Upon successfully passing the CSSLP examination, you must submit a properly completed and executed endorsement form. The endorser attests that the candidate's assertions regarding professional experience are true to the best of their knowledge, and that the candidate is in good standing within the software industry. You will then receive your certificate and ID card. You also become eligible to be listed in the CSSLP Directory, can elect to participate in the Speakers' Bureau, serve on (ISC)[2] committees and participate in its annual elections. You will also be entitled to the full member benefits package.

Maintenance Requirements

Recertification is required every three years, with ongoing requirements to maintain your credentials in good standing. This is primarily accomplished through earning 90 continuing professional education (CPE) credits every three years, with a minimum of 15 CPEs earned each year after certification. CSSLPs must also pay an annual maintenance fee (AMF) of USD100 per year.

For more information on the CSSLP certification, visit **www.isc2.org/csslp-certification**.

(ISC)[2] is the premier not-for-profit organization dedicated to certifying information security professionals around the world. With tens of thousands of credentialed specialists worldwide, (ISC)[2] is dedicated to helping both the certified individual and their organization be successful in the application or information security industry. Indeed, our credentials are considered the Gold Standard in information security. So (ISC)[2] is the logical first contact for anyone serious about protecting information assets at an unsurpassed level of excellence.

CLP000.0
(07/09)