

It's time you addressed the holes in software development

(ISC)²



Certified Secure Software Lifecycle Professional

DHS Software Assurance Forum

October, 2008

**Tony Baratta, CISSP-ISSAP,
ISSMP, SSCP**

**(ISC)² Director of
Professional Programs**



(ISC)² Overview & Background

- Global leaders in certifying and educating information security professionals with the CISSP[®] and related concentrations, CAP[®] and SSCP[®].
- Established in 1989 – not-for-profit consortium of industry leaders.
- More than 60,000 certified professionals in over 135 countries.
- Board of Directors - top information security professionals worldwide.
- All but one of our credentials are accredited ANSI/ISO/IEC Standard 17024 and were the first technology-related credentials to receive this accreditation.



Why Attack Applications?

- Attacking systems became harder
- Perimeter defenses improved
- Attacking applications became easier
- Applications designed without security in mind became more vulnerable and more exploitable



Why Are Applications Vulnerable?

- You can fill in the blanks
 - Applications are vulnerable because
 - _____
 - _____
 - _____



Current Snapshot of Professionalism Efforts. What is the Answer?

- No single answer
- Variety of solutions
- The following are addressing software development in a variety of ways:
 - **IEEE:** CSDA and CSDP (Software development)
 - **SANS:** GSSP-C, GSSP-J (Language specific/secure coding)
 - **ISSECO:** CSSE (Entry level education program with certificate of completion given by iSQI)
 - **DHS:** Software Assurance Initiative (Awareness Program/Forum)
 - **OWASP** – PCP (Web Application Development Security Certification)
 - **Vendor-Specific** (ex: Microsoft, Symantec) based on internal lifecycle processes/technology specific
- There is no indication that these organizations are addressing the content areas in the same holistic manner as (ISC)².



The (ISC)² Approach – The CSSLP?

- Certified Secure Software Lifecycle Professional (CSSLP)
- Base credential (no other certification is required as a prerequisite)
- Professional certification program
- Addresses security in the software lifecycle
- Takes a holistic approach to security in the software lifecycle
- Tests candidates competency (KSAs) to significantly mitigate the security concerns

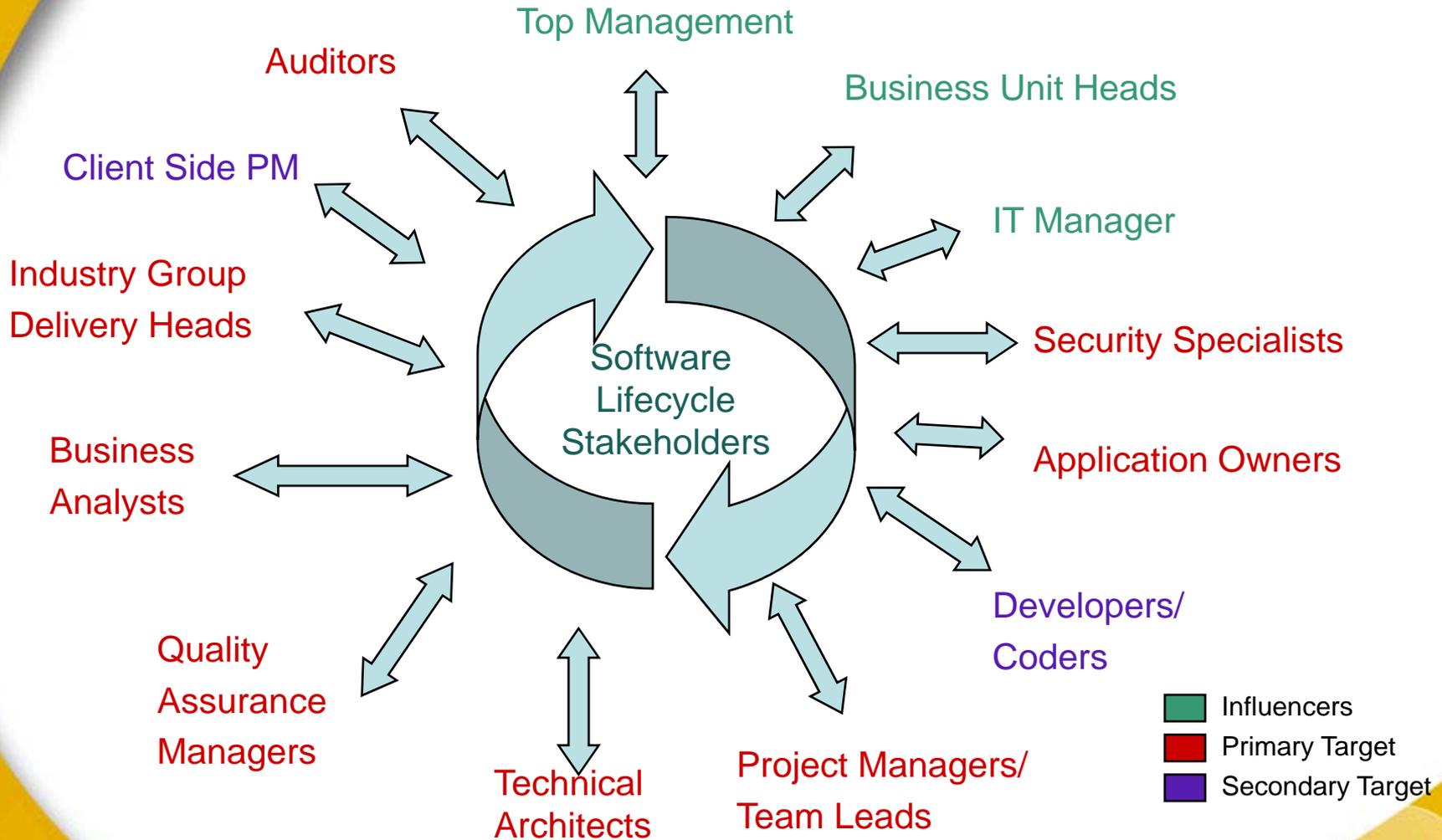


Purpose

- The purpose of the Certification is to provide a credential that speaks to the individual's ability to contribute to the delivery of secure software through the use of best practices.
- The target professionals for this Certification would be those who are involved in the Software Life Cycle activities.



Overview of (ISC)² Software Assurance Certification





Market Drivers

- Secure software and software assurance has emerged as a global concern
- Off shoring of software development
- Desire to minimize design flaws
- Desire to minimize the potential for human error
- Software is not developed with security in mind
- Desire to meet growing industry needs



Certified System Security Lifecycle Professional Scope

(ISC)² CSSLP CBK Domains

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment, Operations, Maintenance, and Disposal



CSSLP Certification Requirements

By Experience Assessment:

- Open through 3/30/09
- May be completed on-line only
- Candidate must submit:
 - Experience Assessment Application
 - Detailed resume of experience
 - Four (4) essays detailing experience in four (4) of the following knowledge areas
 - Fee of \$650 with submission of applications
 - Complete the endorsement process
- Anyone who does not pass the experience assessment will be eligible to receive a free exam voucher



CSSLP Certification Requirements

By Examination:

- The first public exam will be held at the end of June 2009
- Candidate must submit:
 - Completed examination registration form
 - Proof of 4 years experience in the Software Development Lifecycle (SDLC) Process or 3 years experience with a one year waiver for 4-year degree or equivalent in an IT related field
 - Pay a Fee of \$549 early-bird and \$599 standard
- Candidate must
 - Pass the official (ISC)² CSSLP certification examination
 - Complete the endorsement process
- The Associate of (ISC)² Program will apply to those who have passed the exam but need to acquire the necessary minimum experience requirements



CSSLP Recertification Requirements

- Pay Annual Maintenance Fee of \$100.00
- Earn and submit a minimum of 15 CPE's annually
- Earn and submit 90 CPE's by the end of the 3-year certification cycle
- Adhere to the (ISC)² Code of Ethics



Future of CSSLP

- Conduct international marketing efforts
- Seek ANSI/ISO/IEC 17024 accreditation
- Perform exam maintenance activities
- Establish an all-encompassing education program



For more information, please contact:

- Vehbi Tasar, (ISC)² Manager of Professional Programs
 - vtasar@isc2.org
 - OR
- Member Support
 - membersupport@isc2.org
 - OR
- Tony Baratta, (ISC)² Director of Professional Programs
 - tbaratta@isc2.org