Update on the CSSLP®

And its Impact on the SDLC Profession

Hart Rossman, CSSLP
Member, (ISC)² Application Security Advisory Board

(ISC)² Built the largest, most comprehensive Software Security Body of Knowledge

(Certified Secure Software Lifecycle Professional)

CSSLP

Incorporated are:

Public Standards:

NIST,OWASP, ISO 2700x, PCI-DSS, etc.

Corporate Best Practices:

Symantec, Cisco, Microsoft, Xerox, SRA International, Boeing

Industry Associations and Advisory:

SAFEcode, RSA, SANS, ISSA, BASDA, DSCI (NASSCOM)

Government Standards:

Department of Homeland Security / Software Assurance Initiative

Certified Secure Software Lifecycle Professional (CSSLP) Domains

(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

Current CSSLP Statistics

CSSLP Credential Holders:

- 935 certified
- 250 took the education program in 2010
- 129 sat for the exam in 2010

CSSLP Organizations Demographics:

- Banking
- Aerospace
- Government
- Mobile Phone Manufacturers
- Insurance
- Consulting Firms
- Software Security Companies
- Software Manufacturers

CSSLP Statistics (Cont.)

CSSLP Education Program Reviews:

CSSLP course is consistently being touted as "graduate level material" in written reviews submitted by participants

Course Evaluation Statistics:

5 being 'Excellent' and 1 being 'Poor' (of 203 respondents)

- Avg. Quality of Course Materials: Rated 4.7
- Avg. Quality of Course Instructor: Rated 4.8

CSSLP Statistics (Cont.)

Job Titles of CSSLPs :

- Sr. Software Developer/Analyst/Architect/Engineer
- Application Security Architect/Engineer/Analyst
- Lead Software Engineer
- Project Manager
- CISO
- CSO
- Consultant
- Information Assurance Manager/Analyst/Architect

CSSLP Statistics (Cont.)

Job boards listing CSSLP as required or preferred:

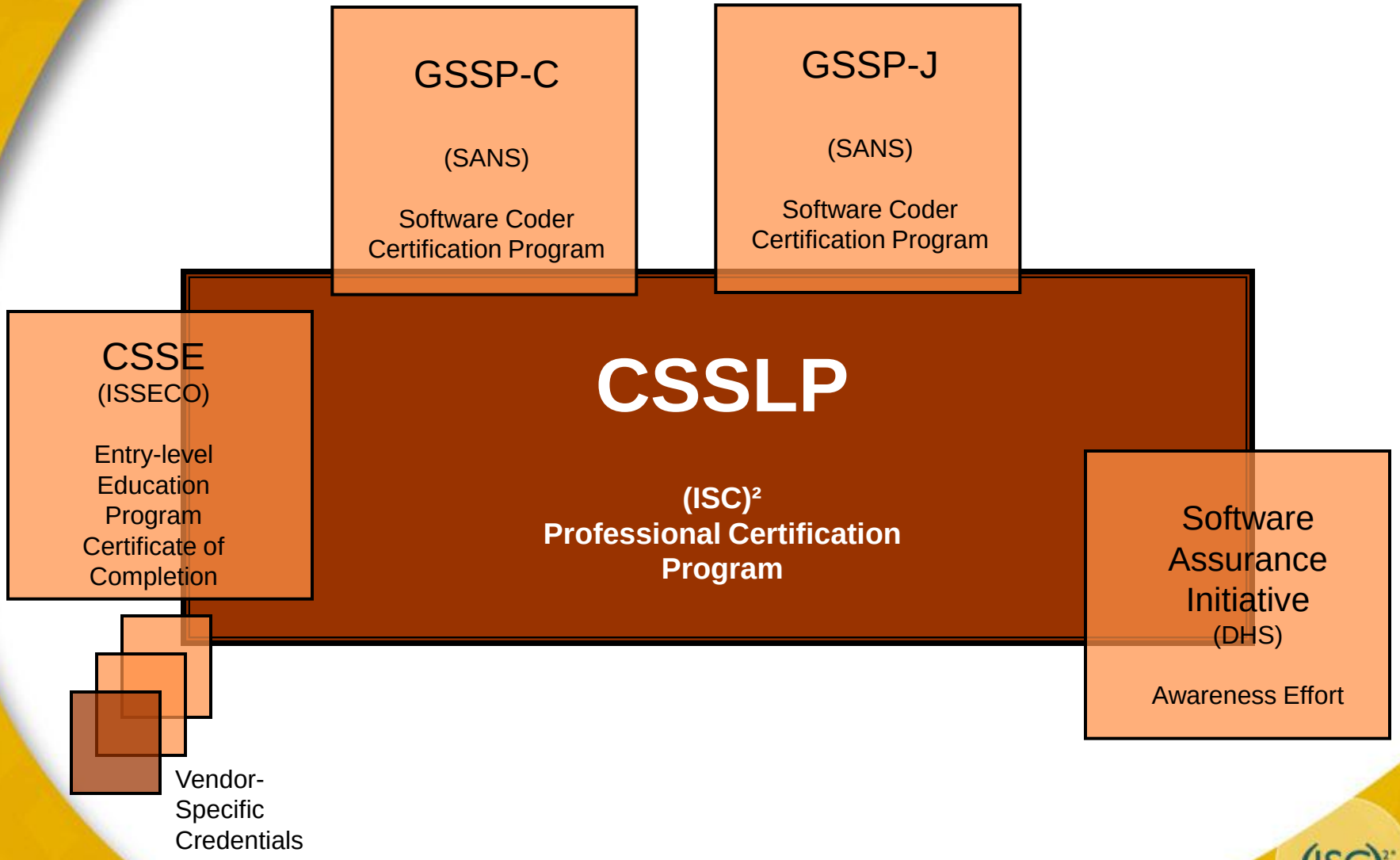
- Chase
- Boeing
- JP Morgan
- Serco
- Dell
- Citi
- EMC
- HP
- Lockheed Martin
- CSC
- Fortify
- Shire Pharmaceutical

How the SwA Community Can Use the CSSLP

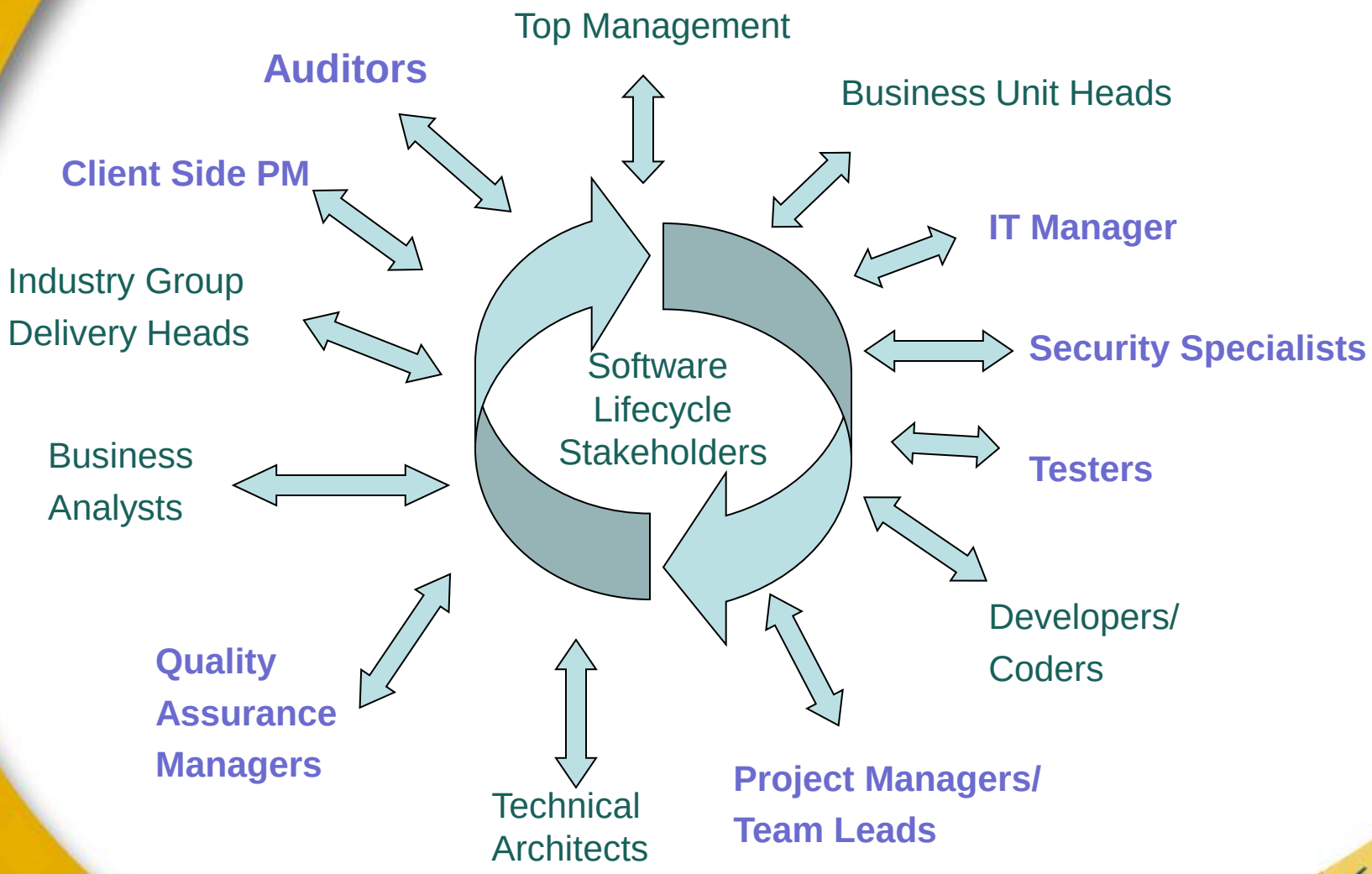
Why the CSSLP?

- Building secure software, along with writing secure code, is critical now!
- Software Assurance has kaleidoscope of perspectives to be factored into secure software lifecycle.
- First line of defense is qualified and educated personnel who know how to write secure code that meets security requirements, including design, testing, deployment, and ultimately disposal of software.

CSSLP CBK® Overlap between Other Certifications/Programs



Software Lifecycle Stakeholder Chart



CSSLP Certification Requirements

By Examination:

- Process
  - Public exams available worldwide through PearsonVUE
  - Candidate must submit:
    - Completed examination registration form
    - Proof of 4 years experience in the Software Development Lifecycle (SDLC) 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) or $599 (standard)
  - Candidate must
    - Pass the official (ISC)²® CSSLP certification examination
    - Complete the endorsement process
    - Maintain their CSSLP status with CPE's

What's Next for the CSSLP?

Progress of the CSSLP

- **ANSI Accreditation Achieved – Oct 2010**
- **(ISC)² Application Security Advisory Board – Established Nov 2010**

• **Andreas Fuchsberger**, CISSP-ISSAP, CSSLP, Royal Halloway, University of London, and security, privacy and identity standards lead, Microsoft Corp.
• **Sharon Hagi**, CISSP, CSSLP, **IBM**
• **Paco (Brian) Hope**, CISSP, CSSLP, **Cigital**
• **Ajoy Kumar**, CSSLP, **JP Morgan Chase**
• **Robert Lai**, CISSP-ISSAP, ISSEP, CAP, CSSLP, **SAIC**
• **Glenn Leifheit**, CSSLP, **FICO** and ASAB co-chair
• **Anthony Lim**, CSSLP, Asia-Pacific, Rational Software, **Suntec**
• **Alessandro Moretti**, CISSP, CSSLP, **UBS**
• **Dr. Yiannis Pavlosoglou**, **UBS**
• **Hart Rossman**, CSSLP, **SAIC**
• **Bola Rotibi**, CEng, **Creative Intellect Consulting Ltd.**
• **Dave Stender**, CISSP, CAP, CSSLP, **U.S. Internal Revenue Service**
• **Dr. Vehbi Tasar**, CISSP, CSSLP, **(ISC)²** and ASAB co-chair
• **Richard Tychansky**, CISSP-ISSEP, CAP, CSSLP, **Lockheed Martin Corp.**

Further details on the AppSec Advisory Board can be found at
https://www.isc2.org/InnerPage.aspx?id=6979&terms=application+security+advisory+board

Future for the CSSLP

- DoD 8570 Mandate Sponsorship Received
- 'Associate' Designation Anticipated
- Working to align the CSSLP curriculum with SEI Cert Undergraduate and Masters level Software Assurance Curriculum Model
- http://www.cert.org/mswa/

For more information, please contact:

David W. Stender, CISSP CSSLP CAP
david.stender@irs.gov

Glenn Johnson, (ISC)²
Corporate Accounts Manager
Lead CSSLP Consultant
gjohnson@isc2.org

Visit www.isc2.org/csslp