Carnegie Mellon University
Software Engineering Institute

# ROADMAP TO SOFTWARE ASSURANCE COMPETENCY

*The CERT Division*

September 2013

Modern society increasingly relies on software systems that put a premium on quality and dependability. The extensive use of the internet and distributed computing has made software security an even more prominent and serious problem. As a result, the interest in and demand for software security specialists have grown dramatically in recent years.

- What background and capability is needed to be a security specialist?
- How do individuals assess their capability and preparation for software security work?
- What is the career path to increased capability and advancement in software development?
- How do employers and acquirers determine their software security needs and assess and improve the software security capabilities of their employees and contractors?

The SEI led development of a software assurance competency framework that supports software security both for organizations and individual specialists. The result is the Software Assurance Competency Model (SwA Model).

## What Knowledge and Capability Is Needed?

As part of earlier work on software assurance education programs, the SEI also led development of an SwA Core Body of Knowledge (CorBoK). The CorBok served as a foundation for the development of curriculum and course guidance for software assurance curricula.

The CorBoK is based on an extensive review of software security reports, books, and articles as well as surveys of and discussions with industry and government SwA professionals. The CorBoK covers the entire spectrum of SwA practices involved in the acquisition, development, operation, and evolution of software systems. Table 1 describes the principal components (knowledge areas) of the CorBoK.

Of course, not every software security job requires knowledge and competency across the entire CorBoK. For example, a position might require deep capability in one or more areas but only a lower level awareness across the other areas. Also, different application domains (e.g., financial system or transportation system) and application types (e.g., web system or embedded system) typically require software security specialists to have additional competencies beyond the CorBoK.

*Table 1: CorBoK Knowledge Areas and Competencies*

| Knowledge Area (KA) | KA Competency |
|---|---|
| Assurance Across Lifecycles | The ability to incorporate assurance technologies and methods into lifecycle processes and development models for new or evolutionary system development, and for system or service acquisition |
| Risk Management | The ability to perform risk analysis and tradeoff assessment, and to prioritize security measures |
| Assurance Assessment | The ability to analyze and validate the effectiveness of assurance operations and create auditable evidence of security measures |
| Assurance Management | The ability to make a business case for software assurance, lead assurance efforts, understand standards, comply with regulations, plan for business continuity, and keep current in security technologies |
| System Security Assurance | The ability to incorporate effective security technologies and methods into new and existing systems |
| System Functionality Assurance | The ability to verify new and existing software system functionality for conformance to requirements and help reveal malicious content |
| System Operational Assurance | The ability to monitor and assess system operational security and respond to new threats |

## What Is the Path to Increased SwA Capability?

Professional competency models typically feature so-called competency levels, which distinguish between what is expected in an entry-level position and what is required in more senior positions. Figure 1 describes SwA competency levels.

The SEI can help organizations develop a SwA competency model that is specific to their organization or their acquisition needs, and identify or develop the associated needed coursework. Contact us for more information.

The SwA Competency Model not only provides the basis for assessing an individual's current competency in software assurance practice, but it can also provide direction to individuals for their professional growth and career advancement.

*The IEEE Computer Society (IEEE-CS) Professional Activities Board (PAB) has endorsed the SEI Software Assurance Competency Model as appropriate for software assurance roles and is consistent with A Framework for PAB Competency Models.*

– Dick Fairley, Chair of the Software and Systems Engineering Committee of the IEEE Computer Society Professional Activities Board (PAB)

Figure 1 outlines the steps in career progression, including guidance on educational preparation and experience expectations. Each level of competency assumes competency at the lower levels. The SwA Competency Model also provides a comprehensive mapping between the SwA CorBoK (knowledge areas and units) and the competency levels.

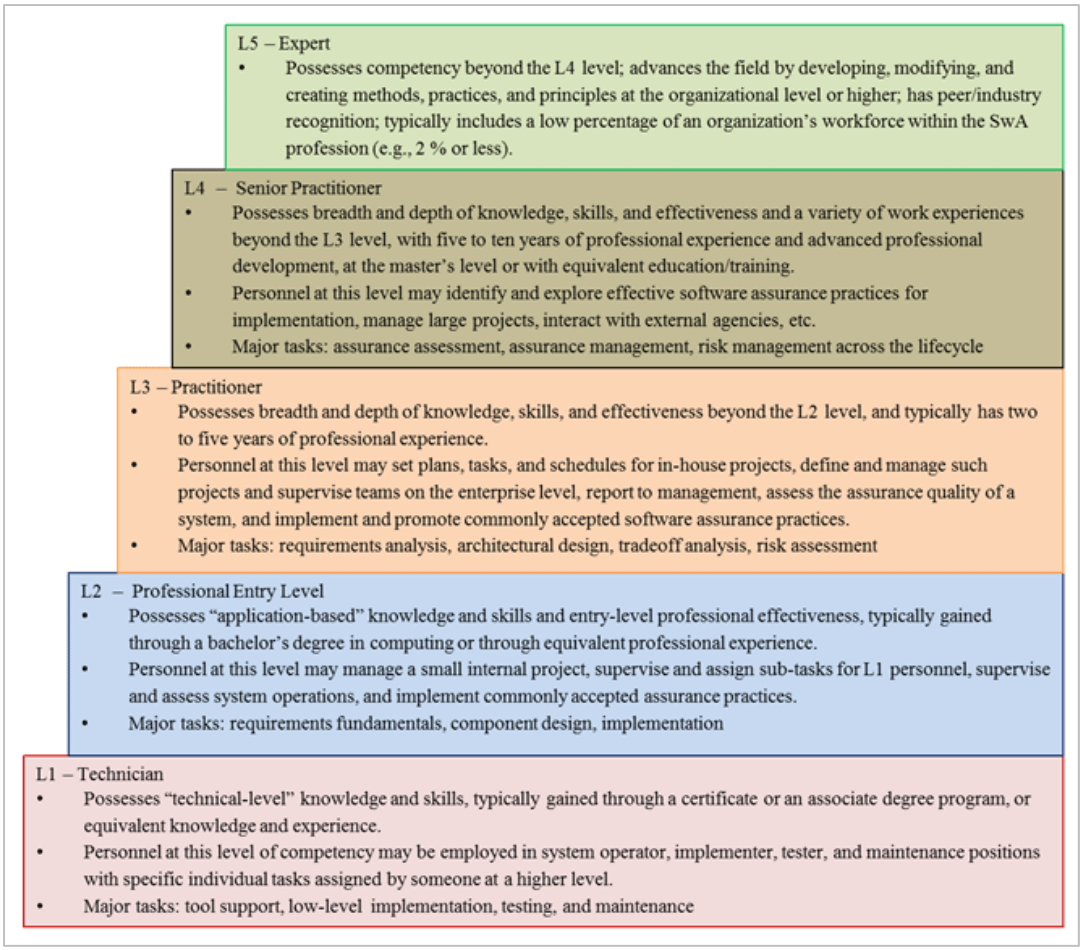


*Figure 1: SwA Competency Levels*

An organization in which software assurance is critical can use the SwA Competency Model for a variety of purposes:

- to structure its software assurance needs and expectations
- to assess the capability of its software assurance personnel
- to provide a roadmap for employee advancement
- to serve as a basis for software assurance professional development plans

The SwA Competency Model was intended to be general enough for individuals or organizations to tailor it easily to their specific employment sector, application domain, or organizational culture.

Of all the participants in recent SEI presentations and webinars on software assurance, only about half had a plan for their own SwA competency development, but more than 80% said they could use the SwA Competency Model in staffing a project.

## Develop Your Own Competency Model

We can help you develop a SwA competency model specific to your needs, and identify or develop the associated needed coursework. Contact us for more information.

## Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

**Phone**: 412/268.5800 | 888.201.4479
**Web**: www.sei.cmu.edu | www.cert.org
**Email**: info@sei.cmu.edu



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.



DM18-0036