**Software Engineering Institute**

# Software Assurance Competency Model

Thomas Hilburn, Embry-Riddle Aeronautical University
Mark Ardis, Stevens Institute of Technology
Glenn Johnson, (ISC)[2]
Andrew Kornecki, Embry-Riddle Aeronautical University
Nancy R. Mead, Software Engineering Institute

**March 2013**

**Carnegie Mellon**

# Table of Contents

# List of Tables

# Acknowledgments

# Abstract

This Software Assurance (SwA) Competency Model was developed to create a foundation for assessing and advancing the capability of software assurance professionals. To help organizations and individuals determine SwA competency across a range of knowledge areas and units, this model provides a span of competency levels 1 through 5, as well as a decomposition into individual competencies based on knowledge and skills. This model also provides a framework for an organization to adapt the model's features to the organization's particular domain, culture, or structure.

# 1 Introduction

## 1.1 Purpose

The Software Assurance (SwA) Competency Model was developed to support the following uses:

- Provide the U.S. Department of Homeland Security (DHS) and other employers of SwA personnel with a means to assess the SwA capabilities of current and potential employees.

- Offer guidance to academic or training organizations that develop SwA courses to support the needs of organizations that are hiring and developing SwA professionals.

- Enhance SwA curricula guidance [Mead 2010a, 2010b, 2011] by providing information about industry needs and expectations for competent SwA professionals.

- Provide direction and a progression for the development and career planning of SwA professionals.

- Provide support for professional certification and licensing activities.

## 1.2 Background

In the development of the SwA Competency Model, a number of competency models and supporting materials were studied and analyzed. The following sources were most influential and useful:

- *Software Assurance Professional Competency Model* (DHS)
  Focuses on 10 SwA specialty areas (e.g., Software Assurance and Security Engineering, and Information Assurance Compliance); describes four levels of behavior indicators for each specialty area [DHS 2012]. The DHS model and the SwA Competency Model described here are compared in Appendix A.

- *Information Technology Competency Model* (Department of Labor)
  Uses a pyramid model to focus on a tiered set of generic non-technical and technical competency areas (e.g., Personal Effectiveness Competencies for Tier 1 and Industry-Wide Technical Competencies for Tier 4). Specific jobs or roles are not designated.

- *A Framework for PAB Competency Models* (Professional Advisory Board [PAB], IEEE Computer Society)
  Provides an introduction to competency models and presents guidelines for achieving consistency among competency models developed by the PAB. A generic framework for a professional that can be instantiated with specific knowledge, skills, and effectiveness levels for a particular computing profession (e.g., Software Engineering practitioner) [PAB 2012a, 2012b]

- *Balancing Software Engineering Education and Industrial Needs*
  Describes a study conducted to help both academia and the software industry form a picture of the relationship between the competencies of recent graduates of undergraduate and graduate software engineering programs and the competencies needed to perform as a software engineering professional [Moreno 2012]

- *Competency Lifecycle Roadmap: Toward Performance Readiness* (Software Engineering Institute)
  Provides an early look at the roadmap for understanding and building workforce readiness. The roadmap includes activities to reach a state of readiness: Assess Plan, Acquire, Validate, and Test Readiness [Behrens 2012].

- Other work on competency models, including works from academia and government [Pyster 2012, Hilburn 1998, NASA 2009, VanLeer 2007]

# 2   SwA Competency Model Features

## 2.1  Terms and Definitions

For the purposes of this model, the following definition of *software assurance* will be used [Mead 2010a]:

> *Application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures.*

In this model, the term *competency* represents the set of knowledge, skills, and effectiveness needed to carry out the job activities associated with one or more roles in an employment position [PAB 2012a]:

- *Knowledge* is what an individual knows and can describe (e.g., can name and define various classes of risks).

- *Skills* are what an individual can do that involves application of knowledge to carry out a task (e.g., can identify and classify the risks associated with a project).

- *Effectiveness* is concerned with the ability to apply knowledge and skills in a productive manner, characterized by attributes of behavior such as aptitude, initiative, enthusiasm, willingness, communication skills, team participation, and leadership.

## 2.2  SwA Competency Levels

Levels of competency are used to distinguish different levels of professional capability, relative to knowledge, skills, and effectiveness. The five levels of SwA competency are characterized as follows [PAB 2012a]:

### L1 – Technician
- Possesses technical knowledge and skills, typically gained through a certificate or an associate degree program, or equivalent knowledge and experience
- May be employed in a system operator, implementer, tester, or maintenance position with specific individual tasks assigned by someone at a higher level
- Main areas of competency: System Operational Assurance, System Functionality Assurance, and System Security Assurance (see Table 1)
- Major tasks: tool support, low-level implementation, testing, and maintenance

### L2 – Professional Entry Level
- Possesses application-based knowledge and skills and entry-level professional effectiveness, typically gained through a bachelor's degree in computing or through equivalent professional experience
- May perform all tasks of L1. May also manage a small internal project; supervise and assign sub-tasks for L1 personnel; supervise and assess system operations; and implement commonly accepted assurance practices

- Main areas of competency: System Functionality Assurance, System Security Assurance, and Assurance Assessment (see Table 1)
- Major tasks: requirements fundamentals, module design, and implementation

### L3 – Practitioner
- Possesses breadth and depth of knowledge, skills, and effectiveness beyond L2, and typically has two to five years of professional experience
- May perform all tasks of L2. May also set plans, tasks, and schedules for in-house projects; define and manage such projects and supervise teams on the enterprise level; report to management; assess the assurance quality of a system; implement and promote commonly accepted software assurance practices
- Main areas of competency: Risk Management, Assurance Assessment, and Assurance Management (see Table 1)
- Major tasks: requirements analysis, architectural design, tradeoff analysis, and risk assessment

### L4 – Senior Practitioner
- Possesses breadth and depth of knowledge, skills, and effectiveness and a variety of work experiences beyond L3, with 5 to 10 years of professional experience and advanced professional development at the master's level or with equivalent education/training
- May perform all tasks of L3. May also identify and explore effective software assurance practices for implementation, manage large projects, interact with external agencies, and so forth
- Main areas of competency: Risk Management, Assurance Assessment, Assurance Management, and Assurance Across Lifecycles (see Table 1)
- Major tasks: assurance assessment, assurance management, and risk management across the lifecycle

### L5 – Expert

Possesses competency beyond L4; advances the field by developing, modifying, and creating methods, practices, and principles at the organizational level or higher; has peer/industry recognition; typically includes a low percentage of an organization's workforce within the SwA profession (e.g., 2 % or less)

## 2.3  SwA Knowledge, Skills, and Effectiveness

The primary source for SwA Competency Model knowledge and skills is the Core Body of Knowledge (CorBoK), contained in *Software Assurance Curriculum Project, Volume I: Master of Software Assurance Reference Curriculum* [Mead 2010a]. The CorBoK consists of the knowledge areas listed in Table 1. Each knowledge area is further divided into second-level units as shown in Table 3. For each unit, competency activities are described for L1-L5.

*Table 1:   CorBoK Knowledge Areas and Competencies*

| Knowledge Area (KA) | KA Competency |
|---|---|
| **AALC:** Assurance Across Lifecycles<br>L3, L4, L5 | 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 |
| **RM:** Risk Management<br>L2, L3, L4, L5 | The ability to perform risk analysis and tradeoff assessment, and to prioritize security measures |
| **AA:** Assurance Assessment<br>L1, L2, L3, L4 | The ability to analyze and validate the effectiveness of assurance operations and create auditable evidence of security measures |
| **AM:** Assurance Management<br>L3, L4, L5 | 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 |
| **SSA:** System Security Assurance<br>L1, L2, L3, L4 | The ability to incorporate effective security technologies and methods into new and existing systems |
| **SFA:** System Functionality Assurance<br>L1, L2, L3 | The ability to verify new and existing software system functionality for conformance to requirements and to help reveal malicious content |
| **SOA:** System Operational Assurance<br>L1, L2, L3 | The ability to monitor and assess system operational security and respond to new threats |

Other than a unit on "Ethics and Integrity" in the System Security Assurance Knowledge Area, the CorBoK does not contain topics on competency associated with effectiveness; the effectiveness attributes are listed in Table 2 (adapted from *A Framework for PAB Competency Models* [PAB 2012a]). In Table 2, for a given attribute, there is no differentiation in effectiveness for the different competency levels; however, professionals would be expected to show an increase in the breadth and depth of capability in these areas of effectiveness as they proceed through their careers and move to higher competency levels.

*Table 2: Competency Attributes of Effectiveness[1]*

| | |
|---|---|
| **Aptitude**<br>L2-L5 | The ability to do a certain software assurance activity at a certain level of competence. Aptitude is not the same as knowledge or skill but rather indicates the ability to apply knowledge in an adept manner. |
| **Initiative**<br>L1-L5 | The ability to start and follow through on a software assurance work activity with interest and determination |
| **Enthusiasm**<br>L1-L5 | Being interested in and excited about performing a software assurance work activity |
| **Willingness**<br>L1-L5 | Undertaking a work activity, when asked, even if it is an activity the individual is not enthusiastic about performing |
| **Communication**<br>L2-L5 | Expressing thoughts and ideas in both oral and written forms in a clear and concise manner while interacting with team members, managers, project stakeholders, and others |
| **Teamwork**<br>L1-L5 | Working professionally and willingly with other team members while collaborating on work activities |
| **Leadership**<br>L3-L5 | Effectively communicating a vision, strategy, or technique that is accepted and shared by team members, managers, project stakeholders, and others |

## 2.4 Competency Designations

Table 3 presents the CorBoK knowledge areas and second-level units, along with a description of the appropriate knowledge and skills for each competency level and the effectiveness attributes. A designation of L1 applies to L1 through L5; a designation of L2 applies to L2 through L5; and so on. The level descriptions indicate the competency activities that are demonstrated at each level.

---

[1] This content was adapted from *A Framework for PAB Competency Models* [PAB 2012a].

*Table 3:    SwA Competency Designations*

| | Knowledge/Skill/Effectiveness | |
|---|---|---|
| **KA** | **Unit** | **Competency Activities** |
| Assurance Across Lifecycles | Software Lifecycle Processes | L1: Understand and execute the portions of a defined process applicable to the assigned tasks.<br>L2: Manage the application of a defined lifecycle software process for a small internal project.<br>L3: Lead and assess process application for small and medium-sized projects over a variety of lifecycle phases, such as new development, acquisition, operation, and evolution.<br>L4: Manage the application of a defined lifecycle software process for a large project, including selecting and adapting existing SwA practices by lifecycle phase.<br>L5: Analyze, design, and evolve lifecycle processes that meet the special organizational or domain needs and constraints. |
| | Software Assurance Processes and Practices | L1: Possess general awareness of methods, procedures, and tools used to assess assurance processes and practices.<br>L2: Apply methods, procedures, and tools to assess assurance processes and practices.<br>L3: Manage integration of assurance practices into typical lifecycle phases.<br>L4: Lead the selection and integration of lifecycle assurance processes and practices in all projects across an organization.<br>L5: Analyze assurance assessment results to determine best practices for various lifecycle phases. |
| Risk Management | Risk Management Concepts | L1: Understand the basic elements of risk management, including threat modeling.<br>L2: Explain how risk analysis is performed.<br>L3: Determine the models, process, and metrics to be used in risk management for small internal projects.<br>L4: Develop the models, processes, and metrics to be used in risk management of projects of any size.<br>L5: Analyze the effectiveness of the use and application of risk management concepts across an organization. |
| | Risk Management Processes | L1: Describe an organizational risk management process.<br>L2: Identify and describe the risks associated with a project.<br>L3: Analyze the likelihood, impact, and severity of each identified risk for a project. Plan and monitor risk management for small to medium-sized projects.<br>L4: Plan and monitor risk management for a large project.<br>L5: Develop a program for analyzing and enhancing risk management practices across an organization. |
| | Software Assurance Risk Management | L1: Describe risk assessment techniques for threats.<br>L2: Apply risk assessment techniques to identified threats.<br>L3: Analyze and plan for mitigation of software assurance risks for small systems.<br>L4: Analyze and plan for mitigation of software assurance risks for both new and existing systems.<br>L5: Assess software assurance processes and practices across an organization and propose improvements. |

| Knowledge/Skill/Effectiveness | | |
|---|---|---|
| **KA** | **Unit** | **Competency Activities** |
| Assurance Assessment | Assurance Assessment Concepts | L1: Provide tool and documentation support for assurance assessment activities.<br>L2: Support assurance assessment activities.<br>L3: Apply various assurance assessment methods (such as validation of security requirements, risk analysis, threat analysis, vulnerability assessments and scans, and assurance evidence) to determine if the software/system being assessed is sufficiently secure within tolerances.<br>L4: Establish and specify the required or desired level of assurance for a specific software application, set of applications, or software-reliant system.<br>L5: Research, analyze, and recommend best practices for assurance assessment methods and techniques. |
| | Measurement for Assessing Assurance | L1: Provide tool and documentation support for assurance assessment measurement.<br>L2: Support assurance assessment measurement activities.<br>L3: Implement assurance assessment measurement activities.<br>L4: Determine and then analyze the key product and process measurements, and performance indicators that can be used to validate the required level of software assurance; determine which software assurance measurement processes and frameworks might be used to accomplish software assurance integration into lifecycle phases.<br>L5: Research, analyze, and recommend best practices for assurance assessment measurement. |
| Assurance Management | Making the Business Case for Assurance | L1: Understand the need for business case analysis.<br>L2: Apply a business case tradeoff analysis to existing data and determine the validity of the case.<br>L3: Identify and gather data needed, and produce the business case.<br>L4: Perform sophisticated business case analysis.<br>L5: Perform research to develop new business case analysis approaches. |
| | Managing Assurance | L1: Understand the importance of assurance in the lifecycle.<br>L2: Support software assurance management tasks.<br>L3: Manage small software assurance projects, building in software assurance practices and measurement.<br>L4: Manage medium-sized to large projects, building in software assurance practices and measurement.<br>L5: Develop new methods for managing assurance. |
| | Compliance Considerations for Assurance | L1: Understand the importance of compliance and possess awareness of laws and regulations.<br>L2: Apply known compliance considerations, laws, and policies to a project.<br>L3: Lead compliance activities for a conventional project.<br>L4: Lead compliance activities for a complex project, and participate in standards and policy activities.<br>L5: Lead standard and policy development activities. Propose new standards and policies. |

| | Knowledge/Skill/Effectiveness | |
|---|---|---|
| **KA** | **Unit** | **Competency Activities** |
| System Security Assurance | For Newly Developed and Acquired Software for Diverse Applications | L1: Possess knowledge of safety and security risks associated with critical infrastructure systems (e.g., banking and finance, energy production and distribution, telecommunications, and transportation systems).<br>L2: Describe the variety of methods by which attackers can damage software or data associated with that software by exploiting weaknesses in the system design or implementation.<br>L3: Apply software assurance countermeasures such as layers, access controls, privileges, intrusion detection, encryption, and code review checklists.<br>L4: Analyze the threats to which software is most likely to be vulnerable in specific operating environments and domains.<br>L5: Perform research on security risks and attack methods, and use it to support modification or creation of techniques used to counter such risks and attacks. |
| | For Diverse Operational (Existing) Systems | L1: Possess knowledge of the attacks that have been used to interfere with an application's or system's operations.<br>L2: Possess knowledge of how gates, locks, guards, and background checks can address risks.<br>L3: Design and plan for access control and authentication.<br>L4: Analyze the threats to which software is most likely to be vulnerable in specific operating environments and domains.<br>L5: Perform research on security risks and attack methods, and use it to support modification or creation of techniques used to counter such risks and attacks. |
| | Ethics and Integrity in Creation, Acquisition, and Operation of Software Systems | L1: Possess knowledge of how people who are knowledgeable about attack and prevention methods are obligated to use their abilities, both legally and ethically.<br>L2: Possess knowledge of the legal and ethical considerations involved in analyzing a variety of historical events and investigations.<br>L3: Follow legal and ethical guidelines in the creation and maintenance of software systems.<br>L4: Play a leadership role in the practice of ethical behavior for software security.<br>L5: Create new case studies for use in education about ethical and legal issues. |
| System Functionality Assurance | Assurance Technology | L1: Possess general awareness of technologies used for system functionality assurance.<br>L2: Apply assurance technology to determine system functionality assurance.<br>L3: Manage integration of selected technology in the functionality assurance process.<br>L4: Select and guide decisions on the use of selected technologies for specific projects.<br>L5: Analyze assurance technologies and contribute to the development of new ones. |
| | Assured Software Development | L1: Understand the importance of assurance in the development process.<br>L2: Engage in the development tasks contributing to functionality assurance.<br>L3: Lead the development of a functionality assurance process in small projects.<br>L4: Select and guide decisions on the use of a specific assurance process in large projects.<br>L5: Analyze assured development processes and contribute to the development of new ones. |

| Knowledge/Skill/Effectiveness | | |
|---|---|---|
| **KA** | **Unit** | **Competency Activities** |
| | Assured Software Analytics | L1: Understand the need for using an analytical approach to software development and the use of supporting tools.<br><br>L2: Apply specific selected methods for structured and functional analysis "in the small."<br><br>L3: Lead projects applying specific selected methods for structured and functional analysis "in the large."<br><br>L4: Lead development teams in testing assurance and developing auditable assurance evidence.<br><br>L5: Develop new methods and techniques allowing for testing assurance, and develop auditable assurance evidence. |
| | Assurance in Acquisition | L1: Understand the need to identify risks in internal software, contracted software, commercial, off-the-shelf (COTS) software, and software as a service (SaaS).<br><br>L2: Define and analyze risks in the acquisition of contracted software, COTS software, and SaaS; employ mitigation tactics to test and identify risks prior to integration.<br><br>L3: Manage multiple supply chains and employ measures to reduce risk in acquisition, and require vendors to employ security measures equal to or greater than internal policy.<br><br>L4: Lead acquisition teams by providing policy, process, tools, and language to prevent the acquisition of insecure software.<br><br>L5: Establish comprehensive policies, plans, and education to L1-L4 personnel, all software development lifecycle stakeholders, and procurement teams to protect against the acquisition of insecure software. |
| System Operational Assurance | Operational Procedures | L1: Understand the role of business objectives and strategic planning in system assurance.<br><br>L2: Support the creation of security policies and procedures for system operations.<br><br>L3: Create security policies and procedures for the operation of a designated system.<br><br>L4: Define the process and procedures for creating security policies and procedures for the operation of a designated system.<br><br>L5: Research, analyze, and recommend best practices for determining security policies and procedures for system operations. |
| | Operational Monitoring | L1: Provide support for the installation and use of tools for monitoring and controlling system operation.<br><br>L2: Support the installation and configuration or acquisition of monitors and controls for systems, services, and personnel.<br><br>L3: Evaluate operational monitoring results with respect to system and service functionality and security, and malicious content and application of countermeasures.<br><br>L4: Lead maintenance and evolution of operational systems while preserving assured functionality and security.<br><br>L5: Research, analyze, and recommend best practices for operational monitoring with respect to system and service functionality and security. |
| | System Control | L1: Provide support for the installation and use of tools for monitoring and controlling system operation.<br><br>L2: Support the implementation of effective responses to operational system accidents, failures, and intrusions.<br><br>L3: Implement effective responses to operational system accidents, failures, and intrusions.<br><br>L4: Lead and plan for effective responses to operational system accidents, failures, and intrusions, including maintenance of business survivability and continuity of operations in adverse environments.<br><br>L5: Research, analyze, and recommend best practices for system control with respect to operational system accidents, failures, and intrusions, including business survivability and continuity of operations in adverse environments. |

# 3 Experience with the Model and Summary

This Software Assurance Competency Model was developed to create a foundation for assessing and advancing the capability of software assurance professionals. To help organizations and individuals determine SwA competency across a range of knowledge areas and units, this model provides a span of competency levels 1 through 5, as well as a decomposition into individual competencies based on knowledge and skills. As noted earlier, this model was compared with the DHS Competency Model in Appendix A. Some mappings of actual organizational positions to the model are shown in Appendix B. This model also provides a framework for an organization to adapt the model's features to the organization's particular domain, culture, or structure.

# Appendix A: Relationship to the DHS Professional Competency Model

The DHS Software Assurance Professional Competency Model had a major influence on the organization and content of the Software Assurance Competency Model described in this report. In this section, we discuss the purpose of the DHS model, its organization of competency areas around specialties, and the associated software assurance competency levels.

## Purpose of Competency Models

The DHS model [DHS 2012] is designed to serve the following needs:

- *Interagency and public-private collaboration to promote and enable security and resilience of software throughout the lifecycle.*
- *Means to reduce exploitable software weaknesses and improve capabilities that routinely develop, acquire, and deploy resilient software products.*
- *Development and publishing of software security content and SwA curriculum courseware focused on integrating software security content into relevant education and training programs.*
- *Software security automation and measurement capabilities.*

Clearly, there is substantial commonality and overlap between the purposes of the two models. The primary distinction is that this model (see Section 1.1) is intended to serve a bit broader spectrum of SwA stakeholders, but it does include the DHS stakeholders as a principal focus.

## Organization of Competency Areas

The DHS organizes its Model around a set of "specialty areas" aligned with the National Initiative for Cybersecurity Education (NICE) that correspond to the range of areas in which the DHS has interest and responsibility:

- Software Assurance and Security Engineering
- Information Assurance Compliance
- Enterprise Architecture
- Technology Demonstration
- Education and Training
- Strategic Planning and Policy Development
- Knowledge Management
- Cyber Threat Analysis
- Vulnerability Assessment and Management
- Systems Requirements Planning

The content of this model is related to the DHS specialty area of Software Assurance and Security Engineering, with additional topics integrated from other specialty areas such as Technology Demonstration, Cyber Threat Analysis, Vulnerability Assessment and Management, and Systems Requirements Planning. The organizational units of this model are "knowledge areas," which correspond to a core body of knowledge developed in an earlier curriculum development project [Mead 2010a].

**SwA Competency Levels**

The DHS model designates four "proficiency" levels for which competencies are specified for each specialty area:

- Level 1 – Basic: Understands the subject matter and is seen as someone who can perform basic or developmental level work in activities requiring this specialty
- Level 2 – Intermediate: Can apply the subject matter and is considered someone who has the capability to fully perform work that requires application of this specialty
- Level 3 – Advanced: Can analyze the subject matter and is seen as someone who can immediately contribute to the success of work requiring this specialty
- Level 4 – Expert: Can synthesize/evaluate the subject matter and is looked to as an expert in this specialty

*Behavioral Indicators*

For each specialty area, the DHS describes, for each level, how the competency manifests itself in observable on-the-job behavior, called *behavioral indicators*.

The four DHS levels correspond well with the top four levels of this model (2-5) (see Section 2.2). This similarity in levels is most prominent in the DHS model's description of behavior indicators for the Software Assurance and Security Engineering specialty area.

The description of each specialty area also designates *proficiency targets* (which identify the proficiency at which a person in a specific career level should be performing) and aligns with the behavioral indicator descriptions for the specialty area. For example, the Software Assurance and Security Engineering specialty area designate the targets depicted in Table 4.

*Table 4:  Proficiency Targets for the Software Assurance and Security Engineering Specialty Area*

| Proficiency Targets | | |
|---|---|---|
| **Project Lead (GS 13)** | **Senior (GS 14)** | **Director (GS 15)** |
| 3 - Advanced | 4 - Expert | 4 - Expert |

Appendix B designates proficiency targets for various software assurance jobs/roles.

# Appendix B: SwA Draft Competency Model Review Result

The tables in this appendix designate proficiency targets for various software assurance jobs and roles.

Table 5:  Proficiency Targets for Various Software Assurance Jobs and Roles

| Technical Level | Title | Behavioral Indicators | Proficiency Target |
|---|---|---|---|
| L1 | Acceptance Tester | 1 - Basic | Entry/Apprentice |
| L1 | Junior Information Assurance Engineer | 1 - Basic | Entry/Apprentice |
| L1 | Programmer 1 | 1 - Basic | Entry/Apprentice |
| L1 | Junior Software Assurance Engineer | 1 - Basic | Entry/Apprentice |
| L1 | Junior Application Security Engineer | 1 - Basic | Entry/Apprentice |
| L1 | Junior Security Engineer | 1 - Basic | Entry/Apprentice |
| L1 | Software Assurance Technician | 1 - Basic | Entry/Apprentice |
| L1 | Software Assurance Engineer | 1 - Basic | Entry/Apprentice |
| L2 | Information Assurance Analyst | 2 - Intermediate | Journey |
| L2 | Information Assurance Engineer | 2 - Intermediate | Journey |
| L2 | Integration Engineer | 2 - Intermediate | Journey |
| L2 | Maintenance Engineer | 2 - Intermediate | Journey |
| L2 | Programmer 2 | 2 - Intermediate | Journey |
| L2 | QA Engineer | 2 - Intermediate  3 - Advanced | Journey |
| L2 | Release Engineer | 2 - Intermediate | Journey |
| L2 | Software Developer | 2 - Intermediate  3 - Advanced | Journey |
| L2 | Software Implementer | 2 - Intermediate  3 - Advanced | Journey |
| L2 | Software Programmer | 2 - Intermediate  3 - Advanced | Journey |
| L2 | Support Engineer | 2 - Intermediate | Journey |
| L2 | Test Engineer | 2 - Intermediate | Journey |
| L2 | Application Security Analyst | 2 - Intermediate  3 - Advanced | Journey |
| L2 | Application Security Engineer | 2 - Intermediate  3 - Advanced | Journey |
| L3 | Application Security Architect | 2 - Intermediate  3 - Advanced | Journey |
| L3 | Consultant | 2 - Intermediate  3 - Advanced | Journey |
| L3 | Consulting Architect | 2 - Intermediate  3 - Advanced | Journey |
| L3 | Consulting Engineer | 2 - Intermediate  3 - Advanced | Journey |
| L3 | Information Assurance Architect | 2 - Intermediate  3 - Advanced | Journey |
| L3 | Programmer 3 | 3 - Advanced | Senior/Master |
| L3 | Requirements Engineer | 2 - Intermediate  3 - Advanced | Journey |

| Technical Level | Title | Behavioral Indicators | Proficiency Target |
|---|---|---|---|
| L3 | Security Control Assessor | 3 - Advanced | Senior/Master |
| L3 | Software Architect | 3 - Advanced | Senior/Master |
| L3 | Software Manager | 2 - Intermediate  3 - Advanced | Journey |
| L3 | Software Team Lead | 3 - Advanced | Senior/Master |
| L3 | Senior Information Assurance Engineer | 3 - Advanced | Senior/Master |
| L3 | Senior Programmer | 3 - Advanced | Senior/Master |
| L3 | Senior Software Analyst | 3 - Advanced | Senior/Master |
| L3 | Senior Software Developer | 3 - Advanced | Senior/Master |
| L3 | Senior Software Engineer | 3 - Advanced | Senior/Master |
| L4 | Information Assurance Manager | 3 - Advanced | Senior/Master |
| L4 | Lead Software Engineer | 3 - Advanced | Senior/Master |
| L4 | Principal Information Assurance Engineer | 4 - Expert | Senior/Master |
| L4 | Principal Software Engineer | 4 - Expert | Senior/Master |
| L4 | Product Manager | 3 - Advanced | Senior/Master |
| L4 | Project Manager | 3 - Advanced | Senior/Master |
| L4 | Senior Software Architect | 4 - Expert | Senior/Master |
| L5 | Chief Information Assurance Engineer | 4 - Expert | Senior/Master |
| L5 | Chief Software Engineer | 4 - Expert | Senior/Master |

*Table 6:    Proposed SWA Competency Mappings from the (ISC)[2] Application Security Advisory Board*

| Knowledge/Skill/Effectiveness | | | Behavioral Indicators |
|---|---|---|---|
| **KA** | **Unit** | **Job Titles** | |
| Assurance Across Lifecycles | Software Lifecycle Processes | L1: Application Security Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Application Security Engineer | 2 - Intermediate<br>3 – Advanced |
| | | L3: Software Architect | 3 - Advanced |
| | | L4: Application Security Architect, Senior Software Architect Information Assurance Architect | 3 - Advanced  4 - Expert |
| | | L5: Software Team Lead, Principal Security Architect | 4 - Expert |
| | Software Assurance Processes and Practices | L1: QA Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: QA Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Senior QA Engineer | 3 - Advanced  4 - Expert |
| | | L4: Lead QA Engineer | 3 - Advanced  4 - Expert |
| | | L5: Principal QA Engineer, QA Engineer Manager | 4 - Expert |
| Risk Management | Risk Management Concepts | L1: Information Assurance Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Analyst 2 | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L4: Information Assurance Architect | 3 - Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Manager | 4 - Expert |
| | Risk Management Process | L1: Information Assurance Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Architect | 3 - Advanced |
| | | L4: Product Manager | 3 - Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Manager | 3 - Advanced  4 - Expert |
| | Software Assurance Risk Management | L1: Information Assurance Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Architect | 3 - Advanced |
| | | L4: Product Manager | 3 - Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Manager | 3 - Advanced  4 - Expert |

| Knowledge/Skill/Effectiveness | | | Behavioral Indicators |
|---|---|---|---|
| KA | Unit | Job Titles | |
| Assurance Assessment | Assurance Assessment Concepts | L1: Information Assurance Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Architect | 3 – Advanced |
| | | L4: Product Manager | 3 – Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Architect | 3 - Advanced  4 - Expert |
| | Measurement for Assessing Assurance | L1: Information Assurance Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Architect | 3 – Advanced |
| | | L4: Product Manager | 3 – Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Architect | 3 - Advanced  4 - Expert |
| | Assurance Assessment Process | L1: Information Assurance Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Architect | 3 – Advanced |
| | | L4: Product Manager | 3 – Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Architect | 3 - Advanced  4 - Expert |
| Assurance Management | Making the Business Case for Assurance | L1: Information Assurance Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Architect | 3 – Advanced |
| | | L4: Product Manager | 3 – Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Architect | 3 - Advanced  4 - Expert |
| | Managing Assurance | L1: Information Assurance Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Architect | 3 – Advanced |
| | | L4: Product Manager | 3 – Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Architect | 3 - Advanced  4 - Expert |

| Knowledge/Skill/Effectiveness | | | Behavioral Indicators |
|---|---|---|---|
| KA | Unit | Job Titles | |
| | Compliance Considerations for Assurance | L1: Information Assurance Analyst, Information Security Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Engineer, Information Security Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Architect, Information Security Architect | 3 - Advanced |
| | | L4: Product Manager | 3 - Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Architect, Lead Information Security Architect | 3 - Advanced  4 - Expert |
| System Security Assurance | For Newly Developed and Acquired Software for Diverse Applications | L1: Software Developer, Software Programmer, QA Analyst, Software Implementer | 2 - Intermediate<br>3 - Advanced |
| | | L2: QA Engineer, Software Engineer, Requirements Engineer, Programmer 1 | 1 - Basic  2 - Intermediate<br>3 - Advanced |
| | | L3: Programmer 2, Programmer 3, QA Lead, QA Engineer 2 | 2 - Intermediate<br>3 - Advanced |
| | | L4: Senior Software Developer, Senior Software Engineer, Senior Software Architect | 3 - Advanced  4 - Expert |
| | | L5: Lead Software Engineer, Lead Software Developer | 3 - Advanced  4 - Expert |
| | For Diverse Operational (Existing) Systems | L1: Software Developer, Software Programmer, QA Analyst, Software Implementer | 2 - Intermediate<br>3 - Advanced |
| | | L2: QA Engineer, Software Engineer, Requirements Engineer, Programmer 1 | 1 - Basic  2 - Intermediate<br>3 - Advanced |
| | | L3: Programmer 2, Programmer 3, QA Lead, QA Engineer 2 | 2 - Intermediate<br>3 - Advanced |
| | | L4: Senior Software Developer, Senior Software Engineer, Senior Software Architect | 3 - Advanced  4 - Expert |
| | | L5: Lead Software Engineer, Lead Software Developer | 3 - Advanced  4 - Expert |
| | Ethics and Integrity in Creation, Acquisition, and Operation of Software Systems | L1: Information Assurance Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Information Assurance Architect | 3 - Advanced |
| | | L4: Product Manager | 3 - Advanced |
| | | L5: Lead Information Assurance Architect, Information Assurance Architect | 3 - Advanced  4 - Expert |

| Knowledge/Skill/Effectiveness | | | Behavioral Indicators |
|---|---|---|---|
| KA | Unit | Job Titles | |
| System Functionality Assurance | Assurance Technology | L1: QA Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: QA Engineer  QA Analyst 2 | 2 - Intermediate<br>3 - Advanced |
| | | L3: Senior QA Engineer QA Engineer 2, QA Analyst 3 | 3 - Advanced |
| | | L4: Lead QA Engineer | 3 - Advanced |
| | | L5: Principal QA Engineer | 4 - Expert |
| | Assured Software Development | L1: Software Developer, Software Programmer, QA Analyst, Software Implementer | 2 - Intermediate<br>3 - Advanced |
| | | L2: QA Engineer, Software Engineer, Requirements Engineer, Programmer 1 | 2 - Intermediate<br>3 - Advanced |
| | | L3: Programmer 2, Programmer 3, QA Lead, QA Engineer 2 | 2 - Intermediate<br>3 - Advanced |
| | | L4: Senior Software Developer, Senior Software Engineer, Senior Software Architect | 3 - Advanced |
| | | L5: Lead Software Engineer, Lead Software Developer | 3 - Advanced  4 - Expert |
| | Assured Software Analytics | L1: Software Developer, Software Programmer, QA Analyst, Software Implementer | 2 - Intermediate<br>3 - Advanced |
| | | L2: QA Engineer, Software Engineer, Requirements Engineer, Programmer 1 | 2 - Intermediate<br>3 - Advanced |
| | | L3: Programmer 2, Programmer 3, QA Lead, QA Engineer 2 | 2 - Intermediate<br>3 - Advanced |
| | | L4: Senior Software Developer, Senior Software Engineer, Senior Software Architect | 3 - Advanced |
| | | L5: Lead Software Engineer, Lead Software Developer | 3 - Advanced |
| | Assurance in Acquisition | L1: Software Developer, Software Programmer, QA Analyst, Software Implementer | 2 - Intermediate<br>3 - Advanced |
| | | L2: QA Engineer, Software Engineer, Requirements Engineer, Programmer 1 | 2 - Intermediate<br>3 - Advanced |
| | | L3: Programmer 2, Programmer 3, QA Lead, QA Engineer 2 | 2 - Intermediate<br>3 - Advanced |
| | | L4: Senior Software Developer, Senior Software Engineer, Senior Software Architect | 3 - Advanced |
| | | L5: Lead Software Engineer, Lead Software Developer | 3 - Advanced |

| Knowledge/Skill/Effectiveness | | | Behavioral Indicators |
|---|---|---|---|
| KA | Unit | Job Titles | |
| System Operational Assurance | Operational Procedures | L1: Software Developer, Software Programmer, QA Analyst, Software Implementer | 2 - Intermediate<br>3 - Advanced |
| | | L2: QA Engineer, Software Engineer, Requirements Engineer, Programmer 1 | 2 - Intermediate<br>3 - Advanced |
| | | L3: Programmer 2, Programmer 3, QA Lead, QA Engineer 2 | 2 - Intermediate<br>3 - Advanced |
| | | L4: Senior Software Developer, Senior Software Engineer, Senior Software Architect | 3 - Advanced |
| | | L5: Lead Software Engineer, Lead Software Developer | 3 - Advanced |
| | Operational Monitoring | L1: Operations Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Operations Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Operations Engineer 2 | 2 - Intermediate<br>3 - Advanced |
| | | L4: Senior Operations Engineer | 3 - Advanced |
| | | L5: Lead Operations Engineer | 3 - Advanced |
| | System Control | L1: Operations Analyst | 2 - Intermediate<br>3 - Advanced |
| | | L2: Operations Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Operations Engineer 2 | 2 - Intermediate<br>3 - Advanced |
| | | L4: Senior Operations Engineer | 3 - Advanced |
| | | L5: Lead Operations Engineer | 3 - Advanced |

*Table 7:  Proposed SWA Competency Mappings from (ISC)$^2$ Application Security Advisory Board Reviewers*

| KA | Unit | Job Titles | Behavioral Indictors |
|---|---|---|---|
| | | **Knowledge/Skill/Effectiveness** | |
| Assurance Across Lifecycles | Software Lifecycle Processes | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | Software Assurance Processes and Practices | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |

| | Knowledge/Skill/Effectiveness | | Behavioral Indictors |
|---|---|---|---|
| **KA** | **Unit** | **Job Titles** | |
| Risk Management | Risk Management Concepts | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | Risk Management Process | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |

| | Knowledge/Skill/Effectiveness | | Behavioral Indictors |
| --- | --- | --- | --- |
| **KA** | **Unit** | **Job Titles** | |
| | Software Assurance Risk Management | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Application Security Analyst, Application Security Engineer, Consultant, Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| Assurance Assessment | Assurance Assessment Concepts | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Application Security Analyst, Application Security Engineer, Consultant, Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |

| | Knowledge/Skill/Effectiveness | | Behavioral Indictors |
| --- | --- | --- | --- |
| KA | Unit | Job Titles | |
| | Measurement for Assessing Assurance | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Application Security Analyst, Application Security Engineer, Consultant, Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | Assurance Assessment Process | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Application Security Analyst, Application Security Engineer, Consultant, Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |

| | Knowledge/Skill/Effectiveness | | Behavioral Indictors |
|---|---|---|---|
| **KA** | **Unit** | **Job Titles** | |
| Assurance Management | Making the Business Case for Assurance | L1: Junior Information Assurance Engineer | 1 - Basic<br>2 - Intermediate |
| | | L2: Information Assurance Analyst, Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Application Security Analyst, Application Security Engineer, Consultant, Consultant Architect, Consulting Engineer, Information Assurance Architect, Requirements Engineer, Software Architect, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Application Security Architect | 3 - Advanced |
| | | L4: Information Assurance Manager, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | Managing Assurance | L1: Acceptance Tester, Junior Information Assurance Engineer | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, QA Engineer, Release Engineer, Software Implementer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | Compliance Considerations for Assurance | L1: Junior Information Assurance Engineer | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer | 2 - Intermediate<br>3 - Advanced |

| Knowledge/Skill/Effectiveness | | | Behavioral Indictors |
|---|---|---|---|
| KA | Unit | Job Titles | |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced 4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| System Security Assurance | For Newly Developed and Acquired Software for Diverse Applications | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic 2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate 3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced 4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | For Diverse Operational (Existing) Systems | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic 2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate 3 - Advanced |

| Knowledge/Skill/Effectiveness | | | Behavioral Indictors |
|---|---|---|---|
| **KA** | **Unit** | **Job Titles** | |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | Ethics and Integrity in Creation, Acquisition, and Operation of Software Systems | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |

| Knowledge/Skill/Effectiveness | | | Behavioral Indictors |
|---|---|---|---|
| **KA** | **Unit** | **Job Titles** | |
| System Functionality Assurance | Assurance Technology | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Consultant, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | Assured Software Development | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Consultant, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |

| Knowledge/Skill/Effectiveness | | | Behavioral Indictors |
|---|---|---|---|
| **KA** | **Unit** | **Job Titles** | |
| System Functionality Assurance | Assurance Technology | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Application Security Analyst, Application Security Engineer, Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | Assurance in Acquisition | L1: Acceptance Tester, Junior Information Assurance Engineer, Programmer 1 | 1 - Basic<br>2 - Intermediate |
| | | L2: Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Application Security Analyst, Application Security Engineer, Consultant, Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |

| Knowledge/Skill/Effectiveness | | | Behavioral Indictors |
|---|---|---|---|
| KA | Unit | Job Titles | |
| System Operational Assurance | Operational Procedures | L1: Junior Information Assurance Engineer | 1 - Basic<br>2 - Intermediate |
| | | L2: Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, QA Engineer, Release Engineer, Support Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Application Security Analyst, Application Security Engineer, Consulting Engineer, Software Manager, Software Team Lead, Senior Information Assurance Engineer | 3 - Advanced |
| | | L4: Information Assurance Manager, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | Operational Monitoring | L1: Junior Information Assurance Engineer | 1 - Basic<br>2 - Intermediate |
| | | L2: Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Programmer 2, QA Engineer, Release Engineer, Software Developer, Software Implementer, Support Engineer, Integration Engineer, Test Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Application Security Analyst, Application Security Engineer, Consultant, Consultant Architect, Consulting Engineer, Information Assurance Architect, Programmer 3, Requirements Engineer, Software Architect, Software Manager, Software Team Lead, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Developer, Senior Software Engineer, Application Security Architect | 3 - Advanced |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer, Product Manager, Project Manager, Senior Software Architect | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |
| | System Control | L1: Junior Information Assurance Engineer | 1 - Basic<br>2 - Intermediate |
| | | L2: Information Assurance Analyst, Information Assurance Engineer, Maintenance Engineer, Support Engineer | 2 - Intermediate<br>3 - Advanced |
| | | L3: Application Security Analyst, Application Security Engineer, Consulting Engineer, Information Assurance Architect, Software Manager, Senior Information Assurance Engineer, Senior Programmer, Senior Software Analyst, Senior Software Engineer, Application Security Architect, Security Control Assessor | 3 - Advanced |

| Knowledge/Skill/Effectiveness | | | Behavioral Indictors |
|---|---|---|---|
| KA | Unit | Job Titles | |
| | | L4: Information Assurance Manager, Lead Software Engineer, Principal Information Assurance Engineer, Principal Software Engineer | 3 - Advanced<br>4 - Expert |
| | | L5: Chief Information Assurance Engineer, Chief Software Engineer | 4 - Expert |

# Bibliography

*URLs are valid as of the publication date of this document.*

**[Behrens 2012]**

Behrens, Sandra G.; Alberts, C.; & Ruefle, R. *Competency Lifecycle Roadmap: Toward Performance Readiness* (CMU/SEI-2012-TN-020). Software Engineering Institute, Carnegie Mellon University, 2012. http://www.sei.cmu.edu/library/abstracts/reports/12tn020.cfm

**[CS 2001]**

Career Space (CS). *Curriculum Development Guidelines: New ICT Curricula for the 21st Century Designing Tomorrow's Education*. Career Space, 2001.
http://www.cedefop.europa.eu/etv/Upload/Information_resources/Bookshop/50/2204_en.pdf

**[DHS 2012]**

U.S. Department of Homeland Security (DHS). *Software Assurance Professional Competency Model*, July 2012.

**[DoD 2012]**

U.S. Department of Defense (DoD). *Information Assurance Workforce Improvement Program,* DoD Directive 8570.01. U.S. Department of Defense, January 24, 2012.
http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

**[DoL 2012]**

U.S. Department of Labor (DoL). *Information Technology Competency Model*. U.S. Department of Labor, Employment and Training Administration, August 2012.

**[Hilburn 1998]**

Hilburn, T., et al. *Software Engineering Competency Study: Final Report*. Federal Aviation Administration, December 1998.

**[Mead 2010a]**

Mead, Nancy R., et al. *Software Assurance Curriculum Project, Volume I: Master of Software Assurance Reference Curriculum* (CMU/SEI-2010-TR-005). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr005.cfm

**[Mead 2010b]**

Mead, Nancy R.; Hilburn, Thomas B.; & Linger, Richard C. *Software Assurance Curriculum Project, Volume II: Undergraduate Course Outlines* (CMU/SEI-2010-TR-019). Software Engineering Institute, Carnegie Mellon University, 2010.
http://www.sei.cmu.edu/library/abstracts/reports/10tr019.cfm

**[Mead 2011]**
Mead, Nancy R.; Hawthorne, Elizabeth K.; & Ardis, Mark. *Software Assurance Curriculum Project, Volume IV: Community College Education* (CMU/SEI-2011-TR-017). Software Engineering Institute, Carnegie Mellon University, 2011.
http://www.sei.cmu.edu/library/abstracts/reports/11tr017.cfm

**[Moreno 2012]**
Moreno, Ana M., et al. "Balancing Software Engineering Education and Industrial Needs." *The Journal of Systems and Software*, *85* (1607-1620): 2012.

**[NASA 2009]**
National Aeronautics and Space Administration (NASA). "NASA's Systems Engineering Competencies." http://www.nasa.gov/offices/oce/appel/pm-development/
pm_se_competency_framework.html (2009).

**[PAB 2012a]**
Professional Advisory Board. *A Framework for PAB Competency Models*. IEEE Computer Society, Draft Version, August 6, 2012.

**[PAB 2012b]**
Professional Advisory Board. *A Competency Model for Software Engineering Practitioners*. IEEE Computer Society, Draft Version, August 6, 2012.

**[Pyster 2012]**
Pyster, A.; Olwell, D. H.; Ferris, T. L. J.; Hutchison, N.; Enck, S.; Anthony, J.; Henry, D.; & Squires, A. (eds.). *Graduate Reference Curriculum for Systems Engineering (GRCSE)*. Hoboken, NJ. Stevens Institute of Technology. http://www.bkcase.org/grcse/grcse-10/ (2012).

**[VanLeer 2007]**
VanLeer, Mary. "Systems Engineering Competency Development," *Proceedings of the 5th Annual Conference on Systems Engineering Research*. Hoboken, N.J., March 14-16, 2007. Stevens Institute of Technology, 2007.

# REPORT DOCUMENTATION PAGE

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, search-ing existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regard-ing this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

| 1. AGENCY USE ONLY (Leave Blank) | 2. REPORT DATE March 2013 | 3. REPORT TYPE AND DATES COVERED Final |
|---|---|---|

| 4. TITLE AND SUBTITLE Software Assurance Competency Model | 5. FUNDING NUMBERS FA8721-05-C-0003 |
|---|---|

**6. AUTHOR(S)**

Thomas Hilburn, Mark Ardis, Glenn Johnson, Andrew Kornecki, Nancy R. Mead

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213 | 8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2013-TN-004 |
|---|---|

| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116 | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER n/a |
|---|---|

**11. SUPPLEMENTARY NOTES**

| 12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS | 12B DISTRIBUTION CODE |
|---|---|

**13. ABSTRACT (MAXIMUM 200 WORDS)**

This Software Assurance (SwA) Competency Model was developed to create a foundation for assessing and advancing the capability of software assurance professionals. To help organizations and individuals determine SwA competency across a range of knowledge are-as and units, this model provides a span of competency levels 1 through 5, as well as a decomposition into individual competencies based on knowledge and skills. This model also provides a framework for an organization to adapt the model's features to the organiza-tion's particular domain, culture, or structure.

| 14. SUBJECT TERMS software assurance, SWA, competency model; SWA competency | 15. NUMBER OF PAGES 43 |
|---|---|

**16. PRICE CODE**

| 17. SECURITY CLASSIFICATION OF REPORT Unclassified | 18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified | 19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified | 20. LIMITATION OF ABSTRACT UL |
|---|---|---|---|