Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

Strengthening the Security Workforce: A Competency and Functional Framework for Information Technology Security Professionals

Ellen Roth-Perreault, *Booz Allen Hamilton* and Brenda Oldfield, *Department of Homeland Security*

September 11 caused America to recognize the need to secure all parts of the nation's critical infrastructure, including information technology. In 2002, the President released the* National Strategy to Secure Cyberspace*, a document that provides direction for strengthening cybersecurity. A key recommendation of the National Strategy to Secure Cyberspace is to build foundations for the development of security certification programs that will be broadly accepted by the public and private sectors. The Department of Homeland Security – National Cyber Security Division (DHS-NCSD) Training and Education Program has been tasked to lead these efforts by effectively articulating the needs of the public and private sector IT security community.

The foundation for the President's recommendation is clear: currently, over one hundred (100) worthwhile, well-regarded IT security certifications exist, and each has been developed using different criteria. It is challenging to identify—with certainty—which certifications validate which workforce competencies and which certifications would be the best choice to confirm or build the strengths of specific types of workers.

To account for this complexity and uncertainty, the Development Team created a competency-based, functional framework that links competencies and functions to IT security roles fulfilled by personnel in the public and private sectors. The proposed IT Security Competency and Functional Framework: (1) articulates the functions that professionals within the IT security workforce perform, in a common format and language; (2) provides a reference against which to compare the content of IT security certifications, which have been developed independently according to various criteria; (3) can be used to substantiate the wide acceptance of already-developed certifications so that they can be leveraged appropriately for workforce development; and (4) provides a content guideline that can be used to guide the development of future certifications. The Framework builds upon the work of established bodies of knowledge, defines key terms and concepts for well-defined competencies, identifies notional security roles, defines four (4) primary functional perspectives, and establishes an IT Security Role, Competency, and Function Matrix to untangle the certification landscape.

I. Introduction

No single event in history has caused the Federal government to place as much emphasis on building a strong IT security workforce as the September 11, 2001 attacks on America. While these attacks did not specifically target the nation's Information Technology (IT) infrastructure, they opened the public's eyes about the capability that terrorist groups and other hostile threats possess to execute complex operations against the myriad of controls we have in place to protect our nation. September 11 caused America to recognize the need to secure all parts of the nation's critical infrastructure, IT included.

In October of 2001, shortly after the 9/11 attacks, President George W. Bush created the President's Critical Infrastructure Protection Board (PCIPB), which now operates within the Department of Homeland Security as the National Infrastructure Advisory Council (NIAC). The PCIPB's charter was to recommend policies and coordinate programs for protecting information systems for critical infrastructure, such as the electrical grid and telecommunications systems. PCIPB was responsible for performing key activities such as: collaborating with the private sector and all levels of government, encouraging information sharing with appropriate stakeholders, and coordinating incident response. All of these activities involve IT security and require qualified professionals to support increasingly tight demands.

Knowing that IT security workforce development was an issue requiring a focused strategy, the PCIPB created the IT Security Certification Working Group (ITSC-WG). This group was tasked to examine possible approaches to establishing a national IT security certification process to develop and sustain a highly skilled IT security workforce in both the public and private sectors.

A key recommendation from the ITSC-WG is addressed in the *National Strategy to Secure Cyberspace* [1]. The *National Strategy* was created to "engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact." It acknowledged that "Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society, the federal government, state and local governments, the private sector, and the American people." In 2003, the DHS-NCSD was established as a national focal point for cyber security and to facilitate implementation of the *National Strategy*.

ISBN 1-933510-96-7/$15.00

DHS-NCSD was created to coordinate cyber security efforts across the nation, articulated as five (5) priorities:

1. Priority I: A National Cyberspace Security Response System
2. Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program
3. Priority III: A National Cyberspace Security Awareness and Training Program
4. Priority IV: Securing Governments. Cyberspace Priority
5. Priority V: National Security and International Cyberspace Security Cooperation

The PCIPB's work was the foundation for the recommendations on IT security certifications listed in Priority III of the Strategy. Specifically, action/recommendation (A/R) 3/9 states:

- *DHS will encourage efforts that are needed to build foundations for the development of security certification programs that will be broadly accepted by the public and private sectors. DHS and other federal agencies can aid these efforts by effectively articulating the needs of the federal IT security community. (A/R 3-9)*

NCSD established the Training and Education (T/E) Program to lead this effort, as well as others in the area of workforce development.

II. Certification Challenges

Since being established in 2003, the T/E Program has worked with the Department of Defense (DoD), academia, and private sector leaders in the IT and information security fields to examine workforce certifications. After an analysis of over one hundred (100) IT security certifications available in the marketplace, the group of analysts concluded that while many worthwhile, well-regarded IT security certifications exist, they were developed using different criteria to conceptualize and characterize their IT security professionals and associated roles. It is challenging to identify—with certainty—which certifications validate which workforce competencies and which certifications would be the best choice to confirm or build the strengths of specific types of workers. This concern has been echoed by many in industry. For example, an article published in 2004 stated that "Navigating the security certification landscape can be dizzying. Simply identifying the vast array of offerings can be time consuming and overwhelming – never mind determining which cert best fits your needs." [2] Resolving concerns such as these has been the goal of the T/E Program's certification-related work.

As a result of the above complexity and uncertainty, the first critical step identified by the T/E Program in 2006 was to assemble a working group from academia, the private sector, and the federal government to develop a competency-based, functional framework that links competencies and functions to IT security roles fulfilled by personnel in the public and private sectors.

The primary goals of the T/E Program effort were to develop a product that:

1. Articulates the functions that professionals within the IT security workforce perform, in a common format and language that conveys the work, rather than the context in which work is performed (i.e., private sector; government: DoD, intelligence community, civil agencies, etc.);
2. Provides a reference against which to compare the content of IT security certifications, which have been developed independently according to different criteria;
3. Can be used to substantiate the wide acceptance of already-developed certifications so that they can be leveraged appropriately for workforce development; and
4. Provides a content baseline that can be used to shape uniform training guidelines as well as the development of future certifications.

The framework would integrate existing training and education resources such as National Institute of Standards and Technology (NIST) documents, Committee on National Security Systems (CNSS) training standards for information assurance (IA), and widely used industry models for describing IT security processes and programs.

III. Methodology

The development of the IT Security Competency and Functional Framework was an iterative process involving close collaboration with Subject Matter Experts (SMEs) from academia, industry, and government. The process followed in preparing the draft Framework is shown in Figure 1-1.

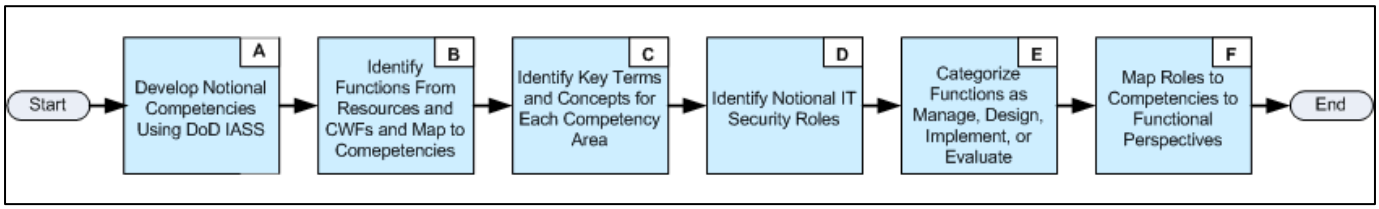

Figure 1-1. IT Security Competency and Functional Framework Development Methodology

1. Data Security	8. Personnel Security
2. Digital Forensics	9. Physical and Environmental Security
3. Enterprise Continuity	10. Procurement
4. Incident Management	11. Regulatory and Standards Compliance
5. IT Security Training and Awareness	12. Risk Management
6. IT Systems Operations and Maintenance	13. Strategic Management
7. Network Security and Telecommunication	14. System and Application Security

Figure 1-2. IT Security Competencies

A. Developing Notional Competencies

The DoD IA Skill Standards document (IASS) was the starting point for deriving IT security competencies. The IASS was developed by the Defense-wide IA Program (DIAP) as part of the DoD 8570.01M-Workforce Improvement Program. DHS-NCSD participated in DoD's working groups that culled public and private sector resources, documents, models, etc. to identify the functions that are performed within the DoD IA workforce. DoD's goal for its own workforce through the IASS is similar to the national level goal of the IT Security Competency and Functional Framework : "to define a common language for describing IA work and work components, in order to provide commercial certification providers and training vendors with targeted information to enhance their learning offerings." The IASS accomplishes this by presenting a set of fifty-six (56) critical IA work functions (noted as CWF in Figure 1-1) and associated tasks that describe DoD work.

To begin creating a framework for DHS-NCSD's product, the Development Team reverse-engineered the IASS document to determine what competencies were represented. The Team took these findings, compared them to other domain-based models of IT security, and ultimately created a list of fourteen discrete competencies (See Figure 1-2). The Team wrote a functional statement/definition for each competency, to clarify the boundaries of what the type of work should be included in each area.

B. Identifying Functions

Once the fourteen competencies were established, the original fifty-six (56) IASS critical work functions were aligned with the competency structure. To identify additional functions for each competency, the Development Team analyzed a multitude of IT security documents, including:

- NIST standards
- CNSS training standards
- International Organization for Standardization (ISO) standards
- Systems Security Engineering Capability Maturity Model (SSE CMM)
- Widely-used private sector models such as Control Objectives for Information and related Technology (COBIT) and the Project Management Body of Knowledge (PMBOK)
- Others.

In all cases, work was captured at the function rather than job task level so that terminology and procedural specificity could be replaced by more general work units that would be universally recognized.

C. Identifying Key Terms and Concepts

The next step entailed identifying key terms and concepts associated with each competency. The key terms and concepts were derived from the same sources as the functions: widely-used documents produced and currently used by the public and private sectors.

The purpose of developing key terms and concepts was to identify the knowledge that professionals should know to be conversant in the field and to perform work functions. Without basic knowledge, no practitioner can operate

competently. In nearly all cases, each key term or concept was assigned to only one competency. In some instances, concepts with impact across IT security were included in multiple areas (i.e., privacy).

The key terms and concepts from all of the competencies make up the Essential Body of Knowledge (EBK) for IT security. At a minimum, individuals should know the key terms and concepts associated with the competencies to which their security role is mapped. A well-rounded individual would have at least basic familiarity with all of the key terms and concepts in the EBK.

D. Identifying Notional IT Security Roles

1. **Chief Information Officer**	6. **Physical Security Specialist**
2. **Chief Security Officer/Chief Information Security Officer**	7. **Privacy Specialist**
3. **Digital Forensics Specialist**	8. **Procurement Specialist**
4. **IT Security Operations and Maintenance Specialist**	9. **IT Security Compliance Officer**
5. **IT Security Specialist**	10. **Security Engineer**

Figure 1-3. IT Security Roles

After a core set of functions were developed for each competency, the Development Team identified a set of ten roles performed by individuals in and adjacent to the IT security field. Again, roles were chosen rather than job titles to eliminate sector-specific language and capture the multitude of positions by function. For example, IT Security Compliance Officer is a role that performs an auditing/evaluation function. Auditor, Compliance Officer, Inspector General, and Inspector are job titles used in various organizations to describe individuals who perform what the Team simply termed the IT Security Compliance Officer role.

E. Categorizing Functions

The Development Team observed that aligning a role with all of the functions within a competency would not necessarily convey the functions a role actually performs. In contrast, each role may perform a certain set of functions within each competency based on the role's responsibilities within the program. For this reason, the Team divided the work functions within each competency into four (4) functional perspectives as follows:

1. **Manage**: Functions that concern high-level oversight and administration of an IT security program.
2. **Design**: Functions that concern development of IT security program or project plans, procedures, and processes.
3. **Implement**: Functions that concern application, implementation, testing, operation, and maintenance of IT security systems, program plans, procedures, and processes.
4. **Evaluate**: Functions that concern assessment or auditing of qualities of an IT security system, process, or work product/deliverable.

It is important to note that the perspectives do *not* convey a lifecycle concept of task or program execution, as is typical of a traditional system development life cycle. The functional perspectives are used to segment the full set of functions within a competency into four (4) categories containing functions of a similar nature.

F. Mapping Roles to Competencies and Functional Perspectives

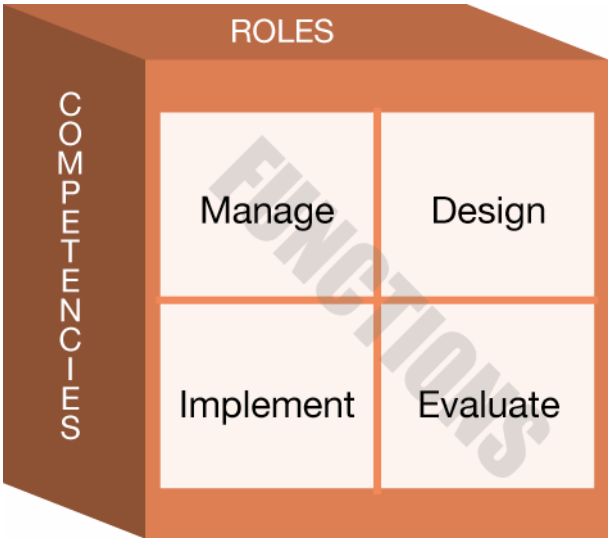

Figure 1-4. Roles-to-Competencies-to-Functions Mapping Diagram

The final step in developing the draft IT Security Competency and Functional Framework was to map roles to appropriate sets of competencies and to identify the specific functional perspective that contains the work that the role would perform. This activity created the IT Security Role, Competency, and Function Matrix. A conceptual, visual depiction of this mapping is shown in Figure 1-4, and the matrix is depicted as Figure 1-5.

IT Security Competency Areas	M - Manage D - Design I - Implement E - Evaluate	IT Security Roles																			
		Chief Information Officer		Chief Information Security Officer/Chief Security Officer		Digital Forensics Specialist		IT Security Compliance Specialist		IT Security Operations and Maintenance Specialist		IT Security Specialist		Physical Security Specialist		Privacy Specialist		Procurement Specialist		Security Engineer	
	1. Data Security	M		M	D								D				D				
									E	I	E	I									E
	2. Digital Forensics			M	D		D														
						I	E		E	I											
	3. Enterprise Continuity	M		M							D		D		D						
									E	I		I		I							
	4. Incident Management	M		M							D		D								
						I			E	I											
	5. IT Security Training and Awareness	M		M									D				D				
									E			I	E								
	6. IT Systems Operations and Maintenance						D			M	D										
						I	E		E	I	E										
	7. Network Security and Telecommunications						D			M	D										
						I			E	I	E										
	8. Personnel Security											M	D								
									E			I				I					
	9. Physical and Environmental Security	M		M										M	D						
									E			I		I	E						
	10. Procurement	M	D	M	D													M	D		
									E									I	E		
	11. Regulatory and Standards Compliance	M		M					D								D				
			E		E			I	E			I				I		I			
	12. Risk Management	M		M									D								
		I	E	I	E	I		I	E	I		I		I		I		I		I	
	13. Strategic Management	M	D	M	D														D		
			E		E				E									I			
	14. System and Application Security	M		M																	D
									E	I										I	E

Figure 1-5. IT Security Role, Competency, and Function Matrix (Draft as of Publication Date)

When a role is mapped to a competency and to a functional perspective within that competency, it means that the role reasonably performs *all* of the functions within the perspective. For example, an IT Security Specialist would have a Design (program scoping and procedure development) role within the Incident Management competency. Therefore, the IT Security Specialist would be mapped to Design functions within the Incident Management competency.

IV. Review Process

In September 2006, DHS-NCSD shared the Development Team's conceptual framework with a focus group of SMEs representing the private sector, government, and academia. The focus group evaluated the framework to ensure that the competencies, their key terms and concepts, and the roles were complete and fully incorporated all aspects of the IT security discipline. Feedback from the focus group was incorporated into the draft framework, which was then presented to a larger working group in October 2006. The working group, which included both IT security generalists and SMEs representing specific roles, reviewed the functional perspectives for each competency and role mapping. This information was compiled to create the first draft for release in December 2006.

DHS-NCSD introduced the first draft to a broader audience of SMEs in January of 2007, including members of the Federal training and education community. The broader review process, which will continue through fall 2007, will leverage professional associations, industry conferences, sector-specific organizations, and the *Federal Register*. Supplementary focus groups of SMEs will be asked to ensure that the respective competencies and functional perspectives are fully representative of the specific role types. DHS-NCSD will aggregate the additional input into the draft by fall of 2007. The IT Security Competency and Functional Framework will then be reevaluated to ensure relevancy and timeliness every two (2) years.

V. Application

For the IT Security Competency and Functional Framework to have the desired impact on certifications, it will need to be utilized in specific ways. If the certification providers want to become part of the DoD Workforce Improvement Program certification schema, they must be accredited by the American National Standards Institute (ANSI), which measures products and processes against the ISO 17024: General Requirements for Bodies Operating Certification of Persons. DHS-NCSD may seek inclusion in the overall accreditation

process by working with ANSI to ask certification providers to identify how their testing objectives map to the IT Security Competency and Functional Framework. Alternatively, DHS-NCSD may pursue other avenues for working with certification providers to identify how certifications map to the content and roles within the Framework.

The federal government, a large customer of the certification industry, could potentially utilize the IT Security Competency and Functional Framework through the Information Systems Security Line of Business (ISS LOB) initiative. The ISS LOB, an interagency program led by the Office of Management and Budget (OMB) and DHS, seeks to streamline specific security projects relevant to all federal agencies including role-based, specialized security training. The IT Security Competency and Functional Framework could be used to identify which competency-based topics would be beneficial for various security roles, therefore helping to shape the federal government's specialized training requirements.

DHS-NCSD strongly believes that the key to addressing the spirit of *National Strategy A/R 3-9* is in clarifying how certification content maps to IT security roles, thereby helping develop broad acceptance of those certifications that are most useful and relevant to the workforce. The unmet certification needs of the federal government and private sector will become clear as certifications are mapped to their target population. Since the Framework will be updated as both the security discipline and technology evolve, it will continue to be a resource for identifying the needs of the public and private sectors.

VI. Conclusion

The premise behind the development of the IT Security Competency and Functional Framework and its role-based mappings is that a one-size-fits-all approach to certification is ineffective if certifications are meant to measure worker competence. IT security work is generally executed by a team of individuals with different responsibilities and spans of control. Therefore, in the IT Security Competency and Functional Framework, individual roles are associated with a subset of competencies and functions, to represent the work performed as part of the IT security team.

The flexibility of the Framework's design enables it to:

1. Be used as a reference against which to compare the content of cyber security certifications, which have been developed independently according to different criteria;
2. Substantiate the wide acceptance of existing certifications so that they can be leveraged appropriately for workforce development; and
3. Provide a content baseline that may be used to guide the development of uniform training guidelines and future certifications.

DHS-NCSD offers the Framework as a product for use across the public and private sectors. The Framework will be revised over time, with input from IT security SMEs, so that it remains a useful, contemporary resource for the community.

VII. References

[1] United States White House. "The National Strategy to Secure Cyber Space" February, 2003.

[2] Tittel, Ed and Lindros, Kim. "Charting a Path Through the Security Certification Landscape" July 14, 2004. http://searchstorage.techtarget.com/tip/0,289483,sid14_gci990011,00.html, Last Accessed: 15 February 2007.