IT Security Essential Body of Knowledge (EBK):

A Competency and Functional Framework for IT Security Workforce Development

Information Security and Privacy Advisory Board Meeting
December 7, 2007

Homeland Security

Training & Education: Program Goals and Objectives

National Strategy to Secure Cyberspace

Priority III:

National Cyberspace Security Awareness and Training Program

NCSD Education and Training Program

Program Goal:

Foster adequate training and education programs to support the Nation's cyber security needs

- Improve cyber security education for IT professionals
- Increase efficiency of existing cyber security training programs
- Promote widely-recognized, vendor-neutral cyber security certifications

Homeland Security

Training & Education: Key Programs

- National Centers of Academic Excellence in Information Assurance Education **- CAEIAE Program**

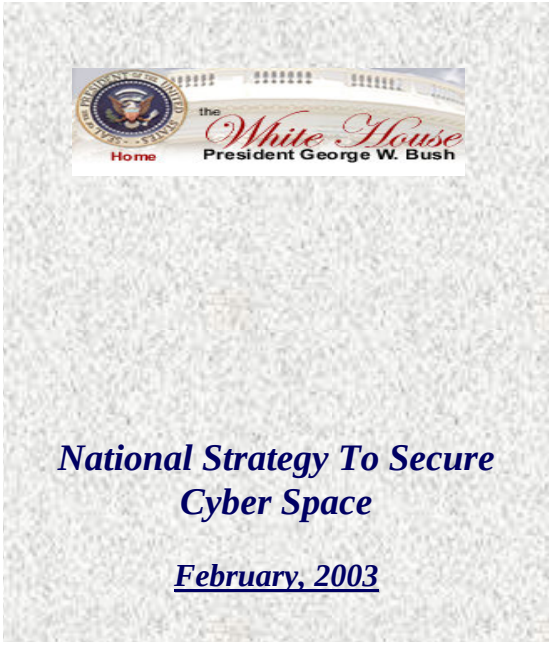
- Federal Cyber Service: Scholarship for Service **- SFS Program**

- **IT Security EBK: A Competency and Functional Framework for IT Security Workforce Development**

Homeland Security

Origin: IT Security Workforce Development Initiative

- **President's Critical Infrastructure Protection Board (PCIPB)**
  IT Security Certification Working Group Recommendations
- **National Infrastructure Advisory Council (NIAC)**
- **National Strategy to Secure Cyberspace, Priority III**



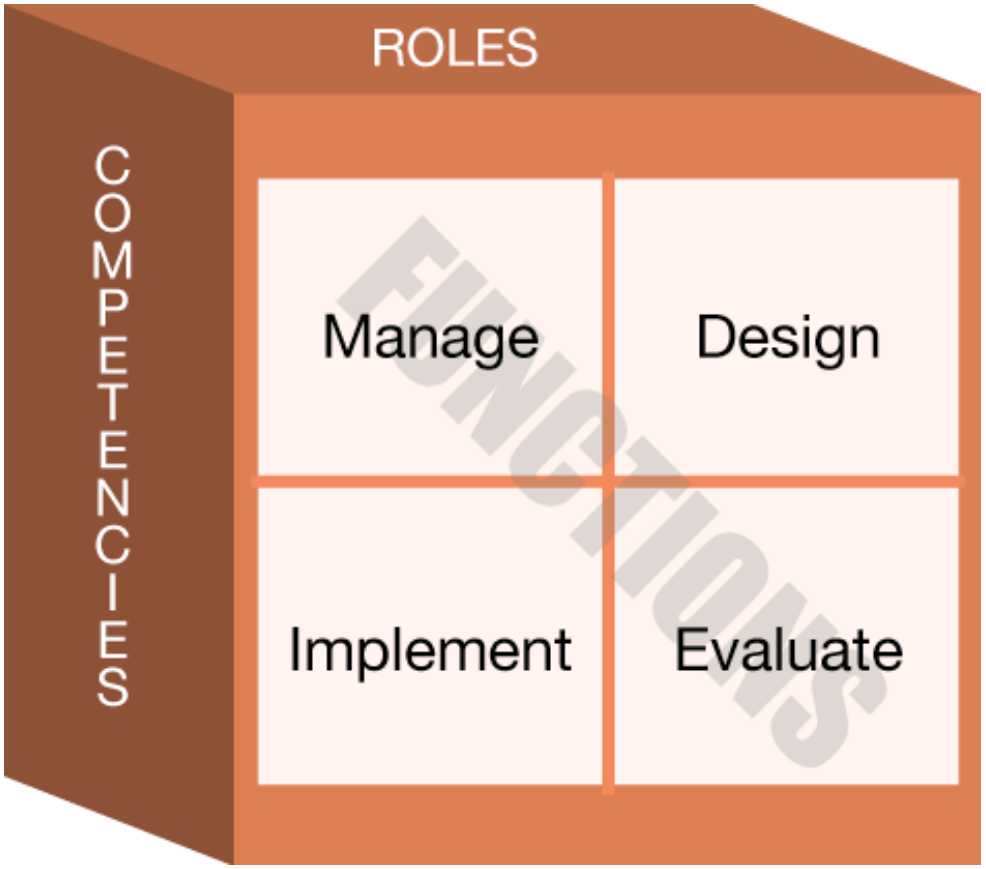
Homeland Security

IT Security EBK: Objectives

- Ensure that we have the most qualified and appropriately trained IT security workforce possible
- Establish a national baseline representing the essential knowledge and skills that IT security practitioners should possess to perform
- Advance the IT security landscape by promoting uniform competency guidelines

Homeland Security

IT Security EBK: Framework Model



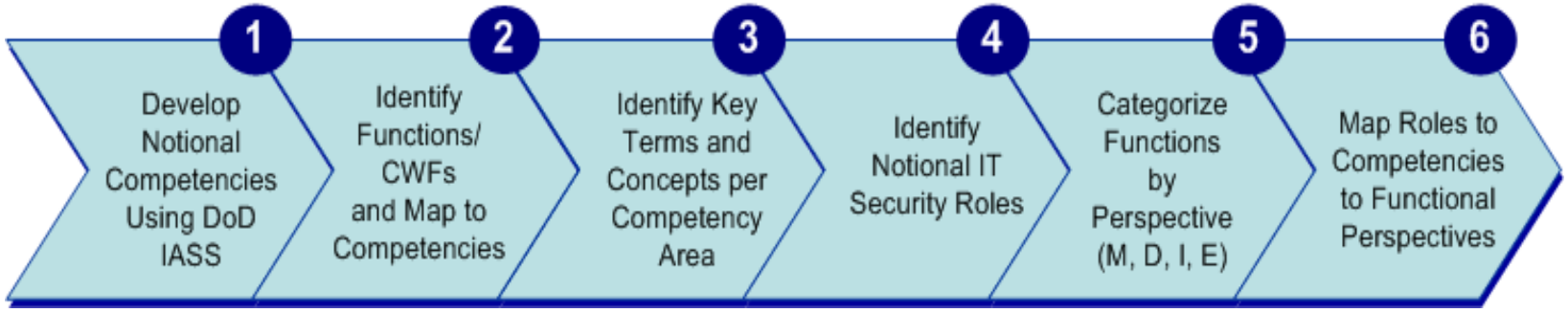
Homeland Security

IT Security EBK: Contributing Resources

- DoD's Workforce Improvement Program (WIP) – Directive 8570.1 IA Training and Certification Framework
- Committee on National Security Systems (CNSS) Training Standards
- DoD Physical and Personnel Security program policy
- Federal Acquisition Regulation
- Various Federal agency program plans
- Position Descriptions
- National Institute of Standards and Technology SP-800 Series
- FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems
- ISO/IEC Standards
- Models (COBIT, SSE-CMM, CMMi)
- Microsoft Operations Framework

Homeland Security

IT Security EBK: Methodology



- Develop notional competencies using DoD IA Skill Standards
- Identify functions from resources and critical work functions (CWFs) and map to competencies
- Identify key terms and concepts for each competency area
- Identify notional IT security roles
- Categorize functions as Manage, Design, Implement, Evaluate
- Map roles to competencies to functional perspectives

Homeland Security

IT Security EBK: Functional Perspectives

	Work functions that concern:
Manage	overseeing a program or technical aspect of a security program at a high level and ensuring its currency with changing risk and threat
Design	scoping a program or developing procedures and processes that guide work execution
Implement	putting programs, processes, or policy into action within an organization
Evaluate	assessing the effectiveness of a program, policy, or process in achieving its objectives

Homeland Security

IT Security EBK: The Framework

- **14 Competency Areas**
  - Definitions to specify parameters and avoid overlap
  - Work functions categorized by functional perspective (M, D, I, E)
- **Key Terms and Concepts**
- **10 Function-Based IT Security Roles**
  - Clusters of organizational positions/jobs
  - Example job titles provided for clarification
  - Role charts illustrate the 3-dimensional model in a useful format

Homeland Security

IT Security EBK: Framework Components

- ✓ 14 Competency Areas
- ✓ Key Terms and Concepts
- ✓ 10 Function-Based IT Security Roles

- Competency, Role and Function Matrix

Homeland Security

IT Security EBK: 14 Competency Areas

- Data Security
- Digital Forensics
- Enterprise Continuity
- Incident Management
- IT Security Training and Awareness
- IT Systems Operations and Maintenance
- Network Security and Telecommunications
- Personnel Security
- Physical and Environmental Security
- Procurement
- Regulatory and Standards
- Risk Management
- Strategic Management
- System and Application Security

Homeland Security

IT Security EBK:
Regulatory and Standards Compliance

Refers to the application of the principles, policies, and procedures that enable an enterprise to meet applicable information security laws, regulations, standards, and policies to satisfy statutory requirements, perform industry-wide best practices, and achieve its information security program goals.

Key Terms and Concepts:

- Assessment
- Auditing
- Certification
- Compliance
- Ethics
- Evaluation
- Governance
- Laws
- Policy
- Privacy Principles/Fair Info Practices
- Procedure
- Regulations
- Security Program
- Standards
- Validation
- Verification

Functions:

- **Manage**: Establish and administer a risk-based enterprise information security program that addresses applicable standards, procedures, directives, policies, regulations and laws
- **Design**: Specify enterprise information security compliance program control requirements
- **Implement**: Monitor and assess the information security compliance practices of all personnel in accordance with enterprise policies and procedures
- **Evaluate**: Assess the effectiveness of enterprise compliance program controls against the applicable laws, regulations, standards, policies, and procedures

IT Security EBK: 10 Roles

- Chief Information Officer
- Digital Forensics Professional
- Information Security Officer/Chief Security Officer
- IT Security Compliance Professional
- IT Security Engineer
- IT Systems Operations and Maintenance Professional
- IT Security Professional
- Physical Security Professional
- Privacy Professional
- Procurement Professional

Homeland Security

IT Security EBK: Role Chart

Role: IT Security Compliance Professional

Role Description:

The IT Security Compliance Professional is responsible for overseeing, evaluating, and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities, encompassing compliance from an internal and external perspective. Such activities include leading and conducting internal investigations, assisting employees comply with internal policies and procedures, and serving as a resource to external compliance officers during independent assessments. The IT Security Compliance Professional provides guidance and autonomous evaluation of the organization to management.

Competencies/Functional Perspectives:

- Data Security: *Evaluate*
- Digital Forensics: *Evaluate*
- Enterprise Continuity: *Evaluate*
- Incident Management: *Evaluate*
- IT Security Training and Awareness: *Evaluate*
- IT Systems Operations & Maintenance: *Evaluate*
- Network Security & Telecommunications: *Evaluate*
- Personnel Security: *Evaluate*
- Physical and Environmental Security: *Evaluate*
- Procurement: *Evaluate*
- Regulatory & Standards Compliance: *Design, Implement, Evaluate*
- Risk Management: *Implement, Evaluate*
- Strategic Management: *Evaluate*
- System and Application Security: Evaluate

Job Titles:

- Auditor
- Compliance Officer
- Inspector General
- Inspector / Investigator
- Regulatory Affairs Analyst

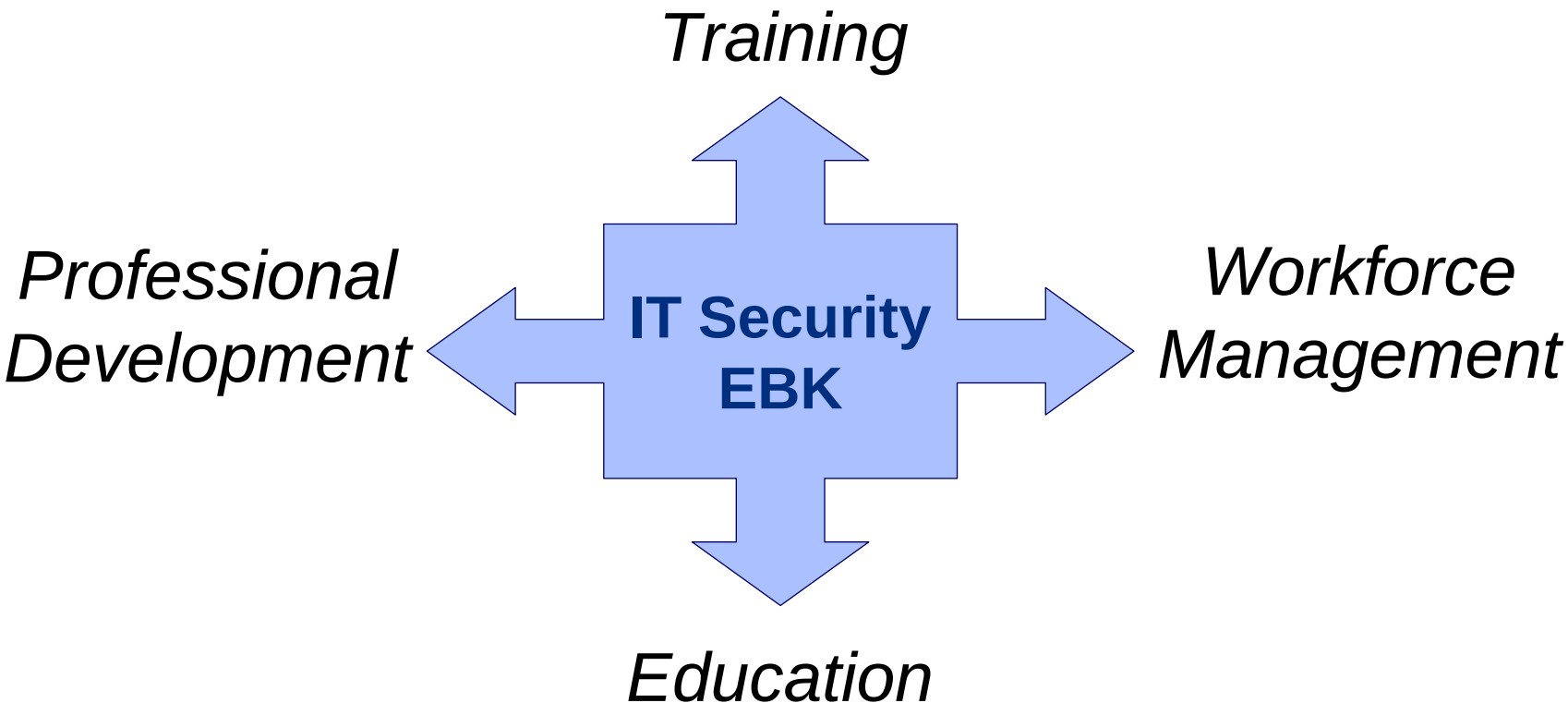
IT Security EBK:

A Competency and Functional Framework for IT Security Workforce Development

Functional Perspectives
M - Manage
D - Design
I - Implement
E - Evaluate

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

IT Security EBK:
Strengthening the IT Security Workforce



Homeland Security

IT Security EBK Testimonials & Federal Register Notice Feedback

"I found this to be an excellent framework with which to move us forward as we continually deal with security issues. Job well done"

- Maryland Judiciary, Administrative Office of the Courts

"The document is well thought out and simple to read. Categories are well done"

- CISSP, Hickman Air Force Base, Hawaii

"It is a very well researched and formatted document that presents a common framework that is greatly needed. I applaud the effort that went into this and hope that it will get traction out there in the greater community"

- BAE Systems

Homeland Security

IT Security EBK Testimonials & Federal Register Notice Feedback

"I commend you all for taking on such a challenge...with numerous security (and now privacy) certifications in the country, it is a real achievement to be able to craft a document as you all have managed to do -- it is not an easy task"

- CEO, SECNAP Network Security (and IBM Data Governance Council)

"This is straight forward, logical, and just downright makes sense. I would love to see this permeate throughout the government."

- SAIC Integrated Security and Systems Solutions

"A good document that is needed in the information security communities. As a developer of Information Security/IA curriculum and as an IT Security Auditor, simple standardization would definitely be a step in the right direction."

- Information Assurance Training Coordinator, Dynetics, Inc.

Homeland Security

Contact Information:

Brenda Oldfield
Program Director
Training and Education
CS&T-National Cyber Security Division

(703) 235-5184
brenda.oldfield@dhs.gov

Homeland Security

Homeland Security