Information Security Workforce Development Matrix Initiative

CIO
COUNCIL

FISSEA 23rd Annual Conference

March 23, 2010

Professionalization of the Workforce

- The CIO Council's IT Workforce Committee partnered with Booz Allen Hamilton to conduct research on the information security environment and to develop role-based information security workforce development matrices

- The matrices are intended to establish a baseline across the Federal Government for staff engaged in information security work

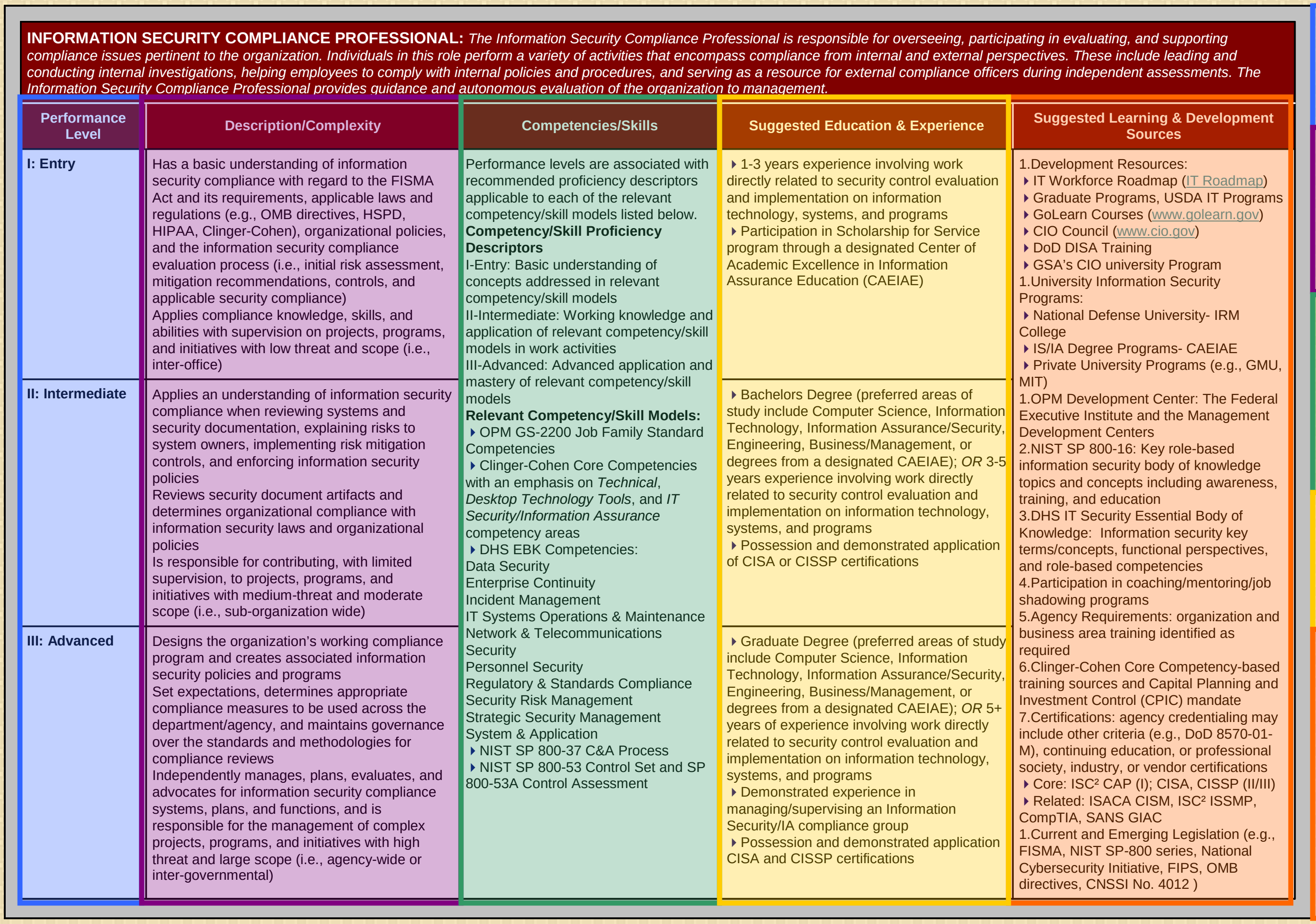
- Provides a government-wide perspective on the types of roles common in information security work and identifies a common framework describing competencies/skills, education, experience, credentials and training needed by performance level

Information Security Roles Identified *(Mar 2010)*

1. Chief Information Security Officer
2. Systems Operations & Maintenance Professional
3. Network Security Specialist
4. Digital Forensics & Incident Response Analyst
5. Information Security Assessor
6. Information Systems Security Officer
7. Security Architect
8. Vulnerability Analyst
9. Information Security Systems & Software Development Specialist
10. Chief Information Officer
11. Information Security Risk Analyst

Components of the IS Matrix

(Matrix below is notional)



INFORMATION SECURITY COMPLIANCE PROFESSIONAL: *The Information Security Compliance Professional is responsible for overseeing, participating in evaluating, and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities that encompass compliance from internal and external perspectives. These include leading and conducting internal investigations, helping employees to comply with internal policies and procedures, and serving as a resource for external compliance officers during independent assessments. The Information Security Compliance Professional provides guidance and autonomous evaluation of the organization to management.*

Performance Level	Description/Complexity	Competencies/Skills	Suggested Education & Experience	Suggested Learning & Development Sources
I: Entry	Has a basic understanding of information security compliance with regard to the FISMA Act and its requirements, applicable laws and regulations (e.g., OMB directives, HSPD, HIPAA, Clinger-Cohen), organizational policies, and the information security compliance evaluation process (i.e., initial risk assessment, mitigation recommendations, controls, and applicable security compliance) Applies compliance knowledge, skills, and abilities with supervision on projects, programs, and initiatives with low threat and scope (i.e., inter-office)	Performance levels are associated with recommended proficiency descriptors applicable to each of the relevant competency/skill models listed below. **Competency/Skill Proficiency Descriptors** I-Entry: Basic understanding of concepts addressed in relevant competency/skill models II-Intermediate: Working knowledge and application of relevant competency/skill models in work activities III-Advanced: Advanced application and mastery of relevant competency/skill models **Relevant Competency/Skill Models:** ▸ OPM GS-2200 Job Family Standard Competencies ▸ Clinger-Cohen Core Competencies with an emphasis on *Technical*, *Desktop Technology Tools*, and *IT Security/Information Assurance* competency areas ▸ DHS EBK Competencies: Data Security Enterprise Continuity Incident Management IT Systems Operations & Maintenance Network & Telecommunications Security Personnel Security Regulatory & Standards Compliance Security Risk Management Strategic Security Management System & Application ▸ NIST SP 800-37 C&A Process ▸ NIST SP 800-53 Control Set and SP 800-53A Control Assessment	▸ 1-3 years experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs ▸ Participation in Scholarship for Service program through a designated Center of Academic Excellence in Information Assurance Education (CAEIAE)	1.Development Resources: ▸ IT Workforce Roadmap (IT Roadmap) ▸ Graduate Programs, USDA IT Programs ▸ GoLearn Courses (www.golearn.gov) ▸ CIO Council (www.cio.gov) ▸ DoD DISA Training ▸ GSA's CIO university Program 1.University Information Security Programs: ▸ National Defense University- IRM College ▸ IS/IA Degree Programs- CAEIAE ▸ Private University Programs (e.g., GMU, MIT) 1.OPM Development Center: The Federal Executive Institute and the Management Development Centers 2.NIST SP 800-16: Key role-based information security body of knowledge topics and concepts including awareness, training, and education 3.DHS IT Security Essential Body of Knowledge: Information security key terms/concepts, functional perspectives, and role-based competencies 4.Participation in coaching/mentoring/job shadowing programs 5.Agency Requirements: organization and business area training identified as required 6.Clinger-Cohen Core Competency-based training sources and Capital Planning and Investment Control (CPIC) mandate 7.Certifications: agency credentialing may include other criteria (e.g., DoD 8570-01-M), continuing education, or professional society, industry, or vendor certifications ▸ Core: ISC^2 CAP (I); CISA, CISSP (II/III) ▸ Related: ISACA CISM, ISC^2 ISSMP, CompTIA, SANS GIAC 1.Current and Emerging Legislation (e.g., FISMA, NIST SP-800 series, National Cybersecurity Initiative, FIPS, OMB directives, CNSSI No. 4012)
II: Intermediate	Applies an understanding of information security compliance when reviewing systems and security documentation, explaining risks to system owners, implementing risk mitigation controls, and enforcing information security policies Reviews security document artifacts and determines organizational compliance with information security laws and organizational policies Is responsible for contributing, with limited supervision, to projects, programs, and initiatives with medium-threat and moderate scope (i.e., sub-organization wide)		▸ Bachelors Degree (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); *OR* 3-5 years experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs ▸ Possession and demonstrated application of CISA or CISSP certifications	
III: Advanced	Designs the organization's working compliance program and creates associated information security policies and programs Set expectations, determines appropriate compliance measures to be used across the department/agency, and maintains governance over the standards and methodologies for compliance reviews Independently manages, plans, evaluates, and advocates for information security compliance systems, plans, and functions, and is responsible for the management of complex projects, programs, and initiatives with high threat and large scope (i.e., agency-wide or inter-governmental)		▸ Graduate Degree (preferred areas of study include Computer Science, Information Technology, Information Assurance/Security, Engineering, Business/Management, or degrees from a designated CAEIAE); *OR* 5+ years of experience involving work directly related to security control evaluation and implementation on information technology, systems, and programs ▸ Demonstrated experience in managing/supervising an Information Security/IA compliance group ▸ Possession and demonstrated application CISA and CISSP certifications	

Level: Categorizes the compliance professional role by proficiency levels required for the position

Description/ Complexity: defines each proficiency level; provides descriptions of the scope of responsibility and experience required for the role at that level

Competencies: Identifies set of measurable knowledge, skills, abilities, and behaviors needed to successfully perform work roles or occupational functions

Suggested Experience: Identifies minimum years of experience required for role

Suggested Education, Training and Development Sources: Provides resources to enhance or develop a job-related knowledge, skill, or ability; provides professional and career development opportunities for an individual in the role

Matrices May Be Used for:

- Recruitment
- Staffing
- Career Planning
- Learning and development
- Performance management
- Succession planning

Draft Matrices Developed to Date

- Information Security Assessor (changed title from Information Security Compliance Professional) – ready to pilot

- Chief Information Security Officer – ready to pilot

- Systems Operations & Maintenance Professional – ready to pilot

- Digital Forensics & Incident Response Analyst – still in development

Next Steps

- Working across the federal government with groups involved in competency efforts
- Spring 2010 - pilot matrices developed so far in several agencies to “road test” prior to implementation
- Post Pilot 2010 - development of additional matrices

Contact:

Dagne Fulcher
Consultant, IT Workforce Issues
703.999.7329

DagneFulcher@verizon.net