FISSEA Workshop Activity Two: Prioritizing the Critical Roles

Information Systems Security Qualifications Matrix: Complexities, Competencies, Experience, and Training

Activity Instructions: For this exercise, you will be evaluating and prioritizing several IT Security roles. Within your group, discuss the prioritization criteria in each section as they exist in your organization. Definitions for each role IT Security role are provided for your reference at the end of this document.

Section I, Important Rating Instructions: Rate each of the IT Security-related roles below using a number from 1 through 7 ***based on the importance of the role*** with respect to IT Security in your organization. Discuss the rationale for prioritizing within your group. Write your findings on this form, and submit your form to the facilitator at the end of today's workshop. *(For remote participants, please email your forms to ascione_david@bah.com.)* Please remember to save and submit your form.

IT Security Role	Importance (1= Highest 7= Lowest)
Chief Information Officer	
Information Security Officer	
IT Security Compliance Officer	
Digital Forensics Professional	
IT Systems Operations and Maintenance Professional	
IT Security Professional	
IT Security Engineer	

1. Explain the criteria you used to determine the importance of the roles with respect to each other.

2. Are there IT Security roles from this list that are not representative of the IT Security roles that exist in your organization? If so, which roles?

3. Are there other IT Security roles in your organization that are missing from the above set of roles? If so, please provide the name and a brief description of the role(s).

4. Other Comments:

FISSEA Workshop Activity Two: Prioritizing the Critical Roles

Information Systems Security Qualifications Matrix: Complexities, Competencies, Experience, and Training

Section II, Qualifications Matrix Need Rating: Rate each of the IT Security-related roles below using a number from 1 through 7 ***based on the role that would benefit THE MOST from the development of an IT Security Qualifications Matrix*** in your organization. If the IT Security Qualifications Matrix were to be implemented in stages to the varying agencies, which roles would be the most critical to work on before the others, based on this priority? Discuss within your group the rationale for prioritizing.

IT Security Roles	Priority (1= Highest 7= Lowest)
Chief Information Officer	
Information Security Officer	
IT Security Compliance Officer	
Digital Forensics Professional	
IT Systems Operations and Maintenance Professional	
IT Security Professional	
IT Security Engineer	

1. Explain the rationale behind the Qualifications Matrix Need ratings you have made.

Section III, Workforce Size Rating Instructions: Rate each of the IT Security-related roles below using a number from 1 through 7 ***based on the size of the workforce associated with the role*** in your organization.

IT Security Roles	Workforce Size (1= Largest 7= Smallest)
Chief Information Officer	
Information Security Officer	
IT Security Compliance Officer	
Digital Forensics Professional	
IT Systems Operations and Maintenance Professional	
IT Security Professional	
IT Security Engineer	

1. Other Comments:

IT SECURITY ROLE DEFINITIONS

I. Chief Information Officer

The Chief Information Officer (CIO) focuses on information security strategy within an organization and is responsible for the strategic use and management of information, information systems, and IT. The CIO establishes and oversees IT security metrics programs, including evaluation of compliance with corporate policies and the effectiveness of policy implementation. The CIO also leads the evaluation of new and emerging IT security technologies.

Example Job Titles:

- Chief Information Officer (CIO)
- Chief Risk Officer (CRO)

II. Digital Forensics Professional

The Digital Forensics Professional performs a variety of highly technical analyses and procedures dealing with the collection, processing, preservation, analysis, and presentation of computer related evidence, including but not limited to data retrieval, password cracking, and locating hidden or otherwise "invisible" information.

Example Job Titles:

- Certified Computer Examiner
- Digital Forensics Analyst
- Digital Forensics Engineer
- Digital Forensics Practitioner
- Digital Forensics Professional

III. Information Security Officer

The Information Security Officer (ISO) specializes in the information and physical security strategy within an organization. The ISO is charged with the development and subsequent enforcement of the company's security policies and procedures, security awareness program, business continuity and disaster recovery plans, and all industry and governmental compliance issues.

Example Job Titles:

- Cyber Security Officer
- Chief Information Security Officer (CISO)
- Enterprise Security Officer
- Information Security Officer
- Senior Agency Information Security Officer

IV. IT Security Compliance Officer

The IT Security Compliance Officer is responsible for overseeing, 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 IT Security Compliance Officer provides guidance and autonomous evaluation of the organization to management.

Example Job Titles:

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

IT SECURITY ROLE DEFINITIONS (cont.)

V. IT Security Engineer

The Security Engineer applies cross-disciplinary IT security knowledge to build IT systems that remain dependable in the face of malice, error, and mischance.

Example Job Titles:

- Requirements Analyst
- Security Analyst
- Security Architect
- Security Engineer
- Software Architect
- System Engineer

VI. IT Security Professional

The IT Security Professional concentrates on protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Example Job Titles:

- Enterprise Security Architect
- Information Assurance Manager (IAM)
- Information Assurance Security Officer (IASO)
- Information Security Officer (ISO)
- Information Security Program Manager
- Information Systems Security Manager (ISSM)
- Information Systems Security Officer (ISSO)
- Security Program Director

VII. IT Systems Operations and Maintenance Professional

The IT Security Operations and Maintenance Professional ensures the security of information and information systems during the Operations and Maintenance phase of the SDLC.

Example Job Titles:

- Database Administrator
- Directory Services Administrator
- Network Administrator
- Service Desk Representative
- System Administrator
- Technical Support Personnel