FISSEA Workshop Activity One: Painting a Well-Rounded Picture

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

Activity Instructions: For this exercise, we will be examining potential qualifications for the *IT Security Professional*. Within your group, discuss qualifications in each of the designated categories for the IT Security Professional as it exists in your organization. A description of the role of the IT Security Professional, along with examples of job titles, is provided below. List the potential qualifications developed by your group 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 Professional Role Description

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.

Sample Job Titles:

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

IT Security Professional Qualifications Categories

Read through each of the qualification categories and document your content in the space provided. Specific guidance for each category is provided to facilitate your group discussions.

Section I: Proficiency Levels

Are there criteria (formal or informal) that determine the proficiency level of the IT Security Professional in your organization? For example, can you classify the proficiency of the IT Security Professionals in your organization by the scope of the projects they work on or manage, the complexity of the work they perform, the years of experience they have, or the size of the budgets they manage? If so, list the different proficiency levels (e.g., Level I, II, III; Basic, Intermediate, Advanced; Entry-Level, Journeyman, Expert) and describe the criteria that correspond with each level.

Level	Description

Section II: Competencies

A competency is a measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to successfully perform work roles or occupational functions.

A set of competencies aligned to the IT Security Professional role (and associated work functions) are provided in the appendix section of this activity. Do these competencies represent the critical competencies required by IT Security Professionals in your organization? Are there competency requirements for IT Security Professionals in your organization missing from the provided list? If so, please document and define those competencies.

Step 1: Review the attached list of IT Security Professional competencies with your group.
Step 2: Discuss whether the competencies provided are applicable to the IT Security Professional role within your organization. List the 4 most important competencies.
Step 3: Are there critical competencies missing that your organization requires for IT Security Professionals? If so, please list those competencies, and/or additional comments.

Section III: Education

Are there specific educational degrees (e.g. Computer Science, Information Technology) and levels (e.g., BA, MA, PhD) that are associated with IT Security Professionals? If so, what are they? Is there a minimum education level required for this role? What are the desired and/or optimal educational levels? Does the desired/required educational background vary depending upon the proficiency levels defined in Section I? Document the educational experiences (by proficiency level, if applicable) in the space below.

Section IV: Training and Career Development

What training and career development opportunities (formal and informal) are available for IT Security Professionals in your organization? Do these training and development opportunities target any of the critical competencies identified in Section II? If so, which ones? Are there other competencies these training and development opportunities help to build? What are they? Do the training and development opportunities changed based on the proficiency levels identified in Section I? Please describe.

Section V: Certifications

Are there certification recommendations or requirements for IT Security Professionals in your organization? If so, what are they? Do the certifications target particular competency areas? Which ones? Do the recommended certifications change dependent upon the proficiency levels identified in Section I? Please describe.

Section VI: Other

Aside from Proficiency Levels, Competencies, Education, Training & Career Development, and Certifications, are there other categories of education and/or experience that would help to determine the qualifications of an IT Security Professional? If so, please list the additional categories and provide a description of the qualifications associated with each.

IT SECURITY PROFESSIONAL COMPETENCIES & WORK FUNCTIONS

1. Data Security

Refers to application of the principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media (electronic and hardcopy) throughout the data life cycle.

Associated Work Functions:

- Ensure that data classification and data management policies and guidance are issued and updated
- Specify policy and coordinate review and approval
- Ensure compliance with data security policies and relevant legal and regulatory requirements
- Ensure appropriate changes and improvement actions are implemented as required
- Develop data security policies using data security standards, guidelines, and requirements that include privacy, access, retention, disposal, incident management, disaster recovery, and configuration
- Identify and document the appropriate level of protection for data
- Specify data and information classification, sensitivity, and need-to-know requirements by information type
- Create authentication and authorization system for users to gain access to data by assigned privileges and permissions
- Develop acceptable use procedures in support of the data security policy
- Develop sensitive data collection and management procedures in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Identify an appropriate set of information security controls based on the perceived risk of compromise to the data
- Develop security testing procedures
- Assess the effectiveness of enterprise data security policies, processes, and procedures against established standards, guidelines, and requirements, and suggest changes where appropriate
- Evaluate the effectiveness of solutions implemented to provide the required protection of data
- Review alleged violations of data security and privacy breaches
- Identify improvement actions required to maintain the appropriate level of data protection

2. Enterprise Continuity

Refers to application of the principles, policies, and procedures used to ensure that an enterprise continues to perform essential business functions after the occurrence of a wide range of potential catastrophic events.

Associated Work Functions:

- Review test, training, and exercise results to determine areas for process improvement, and recommend changes as appropriate
- Assess the effectiveness of the enterprise continuity program, processes, and procedures, and make recommendations for improvement
- Continuously validate the organization against additional mandates, as developed, to ensure full compliance
- Collect and report performance measures and identify improvement actions
- Execute crisis management tests, training, and exercises

3. Incident Management

Refers to knowledge and understanding of the process to prepare and prevent, detect, contain, eradicate, and recover, and the ability to apply lessons learned from incidents impacting the mission of an organization.

Associated Work Functions:

- Develop the incident management policy, based on standards and procedures for the organization
- Identify services that the incident response team should provide
- Create incident response plans in accordance with security policies and organizational goals
- Develop procedures for performing incident handling and reporting
- Create incident response exercises and penetration testing activities
- Develop specific processes for collecting and protecting forensic evidence during incident response
- Specify incident response staffing and training requirements
- Establish an incident management measurement program
- Assess the efficiency and effectiveness of incident response program activities, and make improvement recommendations
- Examine the effectiveness of penetration testing and incident response tests, training, and exercises
- Assess the effectiveness of communications between the incident response team and related internal and external organizations, and implement changes where appropriate
- Identify incident management improvement actions based on assessments of the effectiveness of incident management procedures

IT SECURITY PROFESSIONAL COMPETENCIES & WORK FUNCTIONS (Cont')

4. IT Security Training and Awareness

Refers to the principles, practices, and methods required to raise employee awareness about basic information security and train individuals with information security roles to increase their knowledge, skills, and abilities.

Associated Work Functions:

- Develop the security awareness and training policy for the IT security training and awareness program
- Define the goals and objectives of the IT security awareness and training program
- Work with appropriate security SMEs to ensure completeness and accuracy of the security training and awareness program
- Establish a tracking and reporting strategy for IT security training and awareness
- Establish a change management process to ensure currency and accuracy of training and awareness materials
- Develop a workforce development, training, and awareness program plan
- Perform a needs assessment to determine skill gaps and identify critical needs based on mission requirements
- Develop new—or identify existing—awareness and training materials that are appropriate and timely for intended audiences
- Deliver awareness and training to intended audiences based on identified needs
- Update awareness and training materials when necessary
- Communicate management's commitment, and the importance of the IT security awareness and training program, to the workforce
- Assess and evaluate the IT security awareness and training program for compliance with corporate policies, regulations, and laws (statutes), and measure program and employee performance against objectives
- Review IT security awareness and training program materials and recommend improvements
- Assess the awareness and training program to ensure that it meets not only the organization's stakeholder needs, but that it is effective and covers current IT security issues and legal requirements
- Ensure that information security personnel are receiving the appropriate level and type of training
- Collect, analyze, and report performance measures

5. Personnel Security

Refers to methods and controls used to ensure that an organization's selection and application of human resources (both employee and contractor) are controlled to promote security. Personnel security controls are used to prevent and detect employee-caused security breaches such as theft, fraud, misuse of information, and noncompliance. These controls include organization/functional design elements such as separation of duties, job rotation, and classification.

Associated Work Functions:

- Establish personnel security processes and procedures for individual job roles
- Establish procedures for coordinating with other organizations to ensure that common processes are aligned
- Establish personnel security rules and procedures to which external suppliers (e.g., vendors, contractors) must conform
- Review effectiveness of the personnel security program, and recommend changes that will improve internal practices and/or security organization-wide
- Assess the relationships between personnel security procedures and organization-wide security needs, and make recommendations for improvement
- Periodically review the personnel security program for compliance with standards, procedures, directives, policies, regulations, and laws (statutes)

IT SECURITY PROFESSIONAL COMPETENCIES & WORK FUNCTIONS (Cont')

6. Physical and Environmental Security

Refers to methods and controls used to proactively protect an organization from natural or man-made threats to physical facilities and buildings, as well as to the physical locations where IT equipment is located or work is performed (e.g., computer rooms, work locations). Physical and environmental security protects an organization's personnel, electronic equipment, and data/information.

Associated Work Functions:

- Identify the physical security program requirements and specifications in relationship to enterprise security goals
- Develop policies and procedures for identifying and mitigating physical and environmental threats to information assets, personnel, facilities, and equipment
- Develop a physical security and environmental security plan, including security test plans and contingency plans, in coordination with other security planning functions
- Develop countermeasures against identified risks and vulnerabilities
- Develop criteria for inclusion in the acquisition of facilities, equipment, and services that impact physical security
- Assess and evaluate the overall effectiveness of physical and environmental security policy and controls, and make recommendations for improvement
- Review incident data and make process improvement recommendations
- Assess effectiveness of physical and environmental security control testing
- Evaluate acquisitions that have physical security implications and report findings to management
- Assess the accuracy and effectiveness of the physical security performance measurement system, and make recommendations for improvement where applicable
- Compile, analyze, and report performance measures

7. 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 information security program goals.

Associated Work Functions:

- Monitor, assess, and report information security compliance practices of all personnel and the IT system in accordance with enterprise policies and procedures
- Maintain ongoing and effective communications with key stakeholders for compliance reporting purposes
- Conduct internal audits to determine if information security control objectives, controls, processes, and procedures are effectively applied and maintained, and perform as expected
- Document information security audit results and recommend remedial action policies and procedures

8. Security Risk Management

Refers to the policies, processes, procedures, and technologies used by an organization to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment, and to manage mitigation strategies that achieve the security needed at an affordable cost.

Associated Work Functions:

- Specify risk-based information security requirements and a security concept of operations
- Develop policies, processes, and procedures for identifying, assessing, and mitigating risks to information assets, personnel, facilities, and equipment
- Develop processes and procedures for determining the costs and benefits of risk mitigation strategies
- Develop procedures for documenting the decision to apply mitigation strategies or acceptance of risk
- Develop and maintain risk-based security policies, plans, and procedures based on security requirements and in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Apply controls in support of the risk management program
- Provide input to policies, plans, procedures, and technologies to balance the level of risk associated with benefits provided by mitigating controls
- Implement threat and vulnerability assessments to identify security risks, and regularly update applicable security controls
- Identify risk/functionality tradeoffs, and work with stakeholders to ensure that risk management implementation is consistent with desired organizational risk posture
- Assess effectiveness of the risk management program, and implement changes where required
- Review the performance of, and provide recommendations for, risk management (e.g., security controls, policies/procedures that make up risk management program) tools and techniques
- Assess residual risk in the information infrastructure used by the organization
- Assess the results of threat and vulnerability assessments to identify security risks, and regularly update applicable security controls
- Identify changes to risk management policies and processes that will enable them to remain current with the emerging risk and threat environment