Information Technology (IT) Security Essential Body of Knowledge (EBK):

A Competency and Functional Framework for IT Security Workforce Development

National Cyber Security Division

October 2007

United States Department of Homeland Security
Washington, D.C. 20528

Table of Contents

1 Introduction

1.1 Overview

Over the past two decades, the evolution of technology has quickened society's transformation to a digital environment. These advances have been nonlinear and sometimes chaotic leading to disparities in the composition of the information technology (IT) workforce. The variation in training, expertise, acumen, and experience is a natural consequence and is found in the myriad of recruiting, education, and retention practices of employers. Since the very beginning of the digital revolution, public and private organizations, leaders, and experts have dedicated significant resources to developing the IT security field of practice, yet disparities remain.

Now more than ever, IT security professionals must be prepared to meet the challenges that exist today and in the future. The convergence of voice and data communications systems, the reliance of organizations on those systems, and the emerging threat of sophisticated adversaries and criminals seeking to compromise those systems underscores the need for well trained, well equipped IT security specialists. Furthermore, the interconnectedness of government and industry through shared infrastructures and services demonstrates the need for a universal understanding across domains of the required roles, responsibilities, and competencies of the IT security workforce.

IT security must be a fundamental strategic driver of an organization's business or mission because it protects against theft and hostile acts, has the potential of enhancing productivity, and can improve organizational function and design. As the IT security field matures, it requires qualified professionals to support increasingly sophisticated security demands. In response to this challenge, the Department of Homeland Security National Cyber Security Division (DHS-NCSD) worked with academia, government, and private sector experts to develop a high level framework that establishes a national baseline representing the essential knowledge and skills that IT security practitioners should possess to perform.

DHS-NCSD developed the IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development as an umbrella document that links competencies and functional perspectives to IT security roles fulfilled by personnel in the public and private sectors. Potential benefits of the IT Security EBK for professional development and workforce management initiatives include:

- Articulating the functions that professionals within the IT security workforce perform, in a context-neutral format and language;
- Promoting uniform competency guidelines to increase the overall efficiency of IT security education, training, and professional development; and
- Providing a content guideline that can be leveraged to facilitate cost-effective professional development of the IT workforce, including future skills training and certifications, academic curricula, or other affiliated human resource activities.

The IT Security EBK reflects the vast contribution of resources to date and builds directly upon the work of established references and best practices from the public and private sectors, which were used in the development process and are reflected within the content of this document. The EBK is not an additional set of guidelines, and it is not intended to represent a standard, directive, or policy by DHS. Instead, it further clarifies key IT security terms and concepts for well-defined competencies, identifies notional security roles, defines four primary functional perspectives, and establishes an IT Security Role, Competency, and Functional Matrix. This effort was launched to advance the IT security training and certification landscape to help ensure that we have the most qualified and appropriately trained IT security workforce possible.

1.2 Background

The President's Critical Infrastructure Protection Board (PCIPB) was established in October of 2001 to recommend policies and to 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 complex 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 developing and sustaining a highly skilled IT security workforce, such as establishing a national IT security certification process.

In 2003, the President released the *National Strategy to Secure Cyberspace*, which provides direction for strengthening cyber security. 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." DHS-NCSD was also established in 2003 to act as a national focal point for cyber security, facilitate the implementation of the National Strategy, and coordinate cyber security efforts across the Nation.

A key recommendation from the PCIPB's ITSC-WG work is addressed in the National Strategy as the foundation for 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.*

DHS-NCSD established the Training and Education (T/E) Program to lead this effort, among others, in the area of IT security workforce development.

1.3 Purpose

The IT Security EBK acknowledges the vast contribution of various stakeholders to IT security training and professional development and seeks to articulate a path to better align those efforts within a unifying framework. For instance, over the last several years, the T/E Program has worked with DoD, academia, and private sector leaders in the IT and information security fields to arrive at the conclusion that while many worthwhile, well-regarded IT security certifications exist, these certifications have been developed according to varying criteria based on the focus of each certifying organization and its own market niche.

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 those individuals serving in various IT security roles. Resolving these concerns has been the goal of the T/E Program's certification-related work. As a result of this complexity and uncertainty, in 2006 the T/E Program assembled a working group from academia, the private sector, and the Federal government to develop a competency-based, functional framework that linked competency areas and functions to IT security roles fulfilled by personnel regardless of sector. The EBK framework provides the following outcomes:

- 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, higher education);
- Provides a reference against which to compare the content of IT security certifications, which have been developed independently according to varying criteria;
- Offers one way to further substantiate the wide acceptance of existing certifications so that they can be leveraged appropriately as credentials; and
- Provides a content guideline that can be used to facilitate cost-effective professional development of the IT workforce, including skills training, academic curricula, or additional human resource activities.

1.4 Scope

The IT Security EBK is a resource that can be used by organizations for workforce development and planning, by certification consumers for personal development, and by other groups as they find it useful within their programs. This draft document is not mandated by existing policy and it should be viewed as a complement to existing, widely-used models for describing IT security processes such as the National Institute of Standards and Technology (NIST) or Committee on National Security Systems (CNSS) guidance on IT security training. These resources were used, along with other widely accepted references from the public and private sectors, during the development process and are reflected within the content of this document. The IT Security EBK framework is intended to conceptualize IT security skill requirements in a new way to address evolving IT security challenges.

DHS-NCSD provides the IT Security EBK as a product for use across the public and private sectors. It will be revised over time, with input from subject matter experts (SMEs), to ensure it remains a useful, contemporary resource for the community.

1.5 Methodology

The development of the competency and functional framework was an iterative process involving close collaboration with SMEs from academia, industry, and government. Figure 1-1 identifies the process followed in preparing the Framework and each step is described below, followed by a description of the IT Security EBK review cycle.

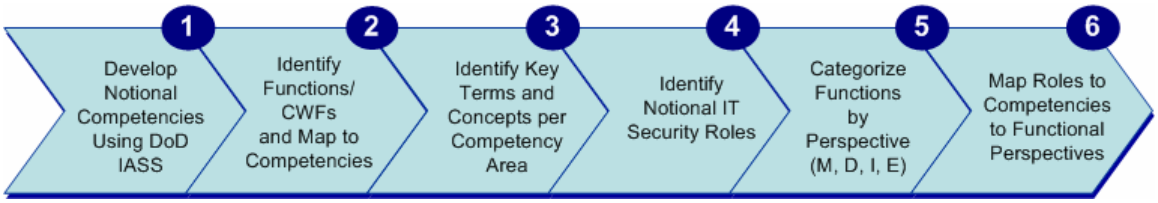

Figure 1-1: Competency and Functional Framework Development Process

Step 1: Develop Notional Competencies Using DoD Information Assurance Skill Standard (IASS). The DoD IASS was a core document used to shape the competency areas and functions captured in the IT Security Competency and Functional Framework. The IASS was developed by the Defense-wide IA Program (DIAP) as part of the DoD 8570-Workforce Improvement Program. DHS-NCSD participated in working groups conducted by DoD in a similar effort of culling public and private sector resources; DoD's goal for its own workforce through the IASS is similar to the national level goal of the IT Security EBK: "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 DoD IASS describes IA work within DoD according to 53 critical work functions (noted as CWF in Figure 1-1), each of which contains multiple tasks. To begin creating a framework for DHS-NCSD, the DoD IASS document was reverse-engineered to arrive at a set of technical competency areas to which the 53 critical work functions and tasks aligned. Each technical competency area was given a functional statement/definition to clarify the boundaries of what would be included in each area.

Step 2: Identify Functions/CWFs and Map to Competencies. Once the competencies were developed, the critical work functions were remapped according to the competency area structure. A multitude of IT security documents were then analyzed to identify additional functions associated with each competency area. These documents included NIST standards, CNSS role-based training standards, International Organization for Standardization (ISO) standards, widely-used private sector models such as Control Objectives for Information and related Technology (COBIT), Systems Security Engineering (SSE) Capability Maturity Model (CMM), and others. Data was captured as functions rather than as job tasks, so that the terminology and procedural specificity of the sector from which the data was gathered could be replaced by more general language that would apply to all sectors.

Step 3: Identify Key Terms and Concepts per Competency Area. This step of development entailed identifying key terms and concepts that represent the knowledge required of professionals to perform the functions within each competency area. The key terms and concepts from all of the competency areas make up the Essential Body of Knowledge (EBK) for IT security (refer to Section 3) which reflects the set of terms, topics, and concepts that one should be familiar with to be a conversant generalist in the IT security field. The scope of professional responsibility of practitioners performing IT security functions varies considerably, and knowledge of key terms and concepts is fundamental to performance. Therefore, individuals should know, at minimum, the key terms and concepts that are part of the competencies to which their role is mapped. In nearly all cases, each key term or concept was assigned to only one competency. In some instances, concepts with wider impact across IT security were included in multiple competencies (e.g., privacy).

Step 4: Identify Notional IT Security Roles. After the competencies were adequately populated with functions based on source document analysis, a set of notional roles performed by individuals in the IT security field were identified. Again, roles were chosen rather than job titles to eliminate sector-specific language and to succinctly capture the multitude of IT security positions in a way that would allow the practitioner to easily identify his or her role. For example, an IT Security Compliance Officer is defined as a role, while the applicable job titles might include auditor, compliance officer, inspector general, or inspector.

Step 5: Categorize Functions by Perspective (Manage, Design, Implement, or Evaluate). After roles were identified, the competencies were revisited and the work functions within each competency were divided into four functional perspectives. 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 (SDLC). The functional perspectives are used to segment the full set of functions within a competency area into four categories containing functions of a similar nature. The functional perspectives are defined as follows:

- **Manage**: Functions that concern overseeing a program or technical aspect of a security program at a high level and ensuring its currency with changing risk and threat.
- **Design**: Functions that concern scoping a program or developing procedures and processes that guide work execution at the program and/or system level.
- **Implement**: Functions that concern putting programs, processes, or policy into action within an organization, either at the program or system level.

- **Evaluate**: Functions that concern assessing the effectiveness of a program, policy, or process in achieving its objectives.

Step 6: Map Roles to Competencies to Functional Perspectives. The final step in developing the 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 Functional Matrix, as illustrated in Section 5. A conceptual, visual depiction of the mapping is shown in Figure 1-2. When a role is mapped to a competency, and to a functional perspective within that competency, it means that the role performs *all* of the functions within the perspective. For example, an IT Security Professional who develops procedures related to incident management is mapped to a Design function within the Incident Management competency area and would perform the work within the Design functional perspective.

The premise behind the mapping and the competency and functional framework is that work conducted by the IT security workforce is complex, and not all work in a given area is performed by a single role. By contrast, the work—from creating the strategy for a component of the IT security program, to developing a program's procedures and scope, to performing hands-on implementation work, to evaluating the work's effectiveness—is performed by a team of individuals with different responsibilities and spans of control. Instead of all roles being responsible for knowing all areas of IT security and being able to perform all job tasks, individual roles are associated with a subset of competencies to represent the work performed as part of the IT security team. The type of work performed is resolved through the four functional perspectives by role across a series of technical competency areas. It is these functions that an individual should be evaluated on if a role-based certification truly measures the ability of a given individual to perform.

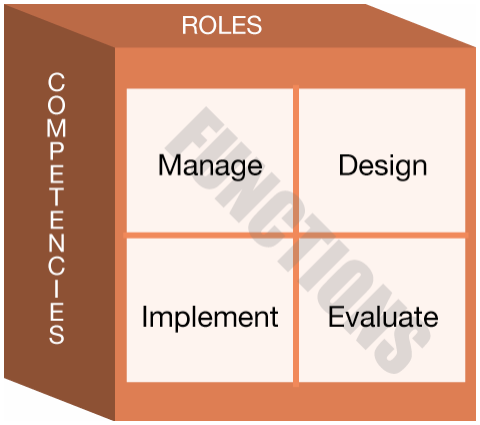

Figure 1-2: Roles to Competencies to Functions Mapping Diagram

Review Cycle. The conceptual framework was shared with focus groups comprised of SMEs representing the private sector, government, and academia. The focus groups analyzed the framework to ensure that the competencies, key terms and concepts, and the roles were complete and fully incorporated all aspects of the IT security discipline. Feedback was incorporated into a draft framework, which was then presented to another larger working group. 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 in December 2006.

DHS-NCSD introduced the first draft to a broader audience of SMEs in January 2007, including members of the Federal training and education community. This activity was followed by a series of supplementary role-based focus groups to ensure that the respective competencies and functional

perspectives fully represent the specific role types. A broader review process will continue through Fall 2007, leveraging professional associations, industry conferences, sector-specific organizations, and the Federal Register for public review and comment. DHS-NCSD will then aggregate the additional input into the IT Security EBK and a final product is expected to be released in Winter 2008. The IT Security EBK: A Competency and Functional Framework for IT Security Workforce Development will then be reevaluated to ensure relevancy and timeliness approximately every two years.

1.6 Organization

The remaining sections of this document are organized as follows:

- ***Section 2: IT Security Competency Areas.*** This section contains the fourteen competency areas, along with their functional statements/definitions and all work functions categorized by four functional perspectives as Manage, Design, Implement, or Evaluate.
- ***Section 3: The IT Security Essential Body of Knowledge.*** This section contains a full, consolidated list of the terms and concepts associated with each IT security competency area. Key Terms and Concepts identify the knowledge that professionals should know to be conversant in the field of IT Security and to perform required work functions.
- ***Section 4: IT Security Roles, Competencies and Functional Perspectives.*** This section includes a listing of the ten roles that characterize the IT security field, as well as the related functional perspectives and competencies. Sample job titles are identified for each role to clarify which job titles align with which role and to allow the individual consumer to identify where his or her role may fit within the framework.
- ***Section 5: IT Security Role, Competency, and Functional Matrix.*** This section contains a visual depiction of the relationship between roles, competencies, and functions clarifying the competencies and perspectives associated with each role.
- ***Appendix: List of Acronyms***. This section lists and defines all of the acronyms contained in the IT Security EBK.

2 IT Security Competency Areas (Definitions and Functions)

This section contains the fourteen competency areas, along with their affiliated functional statements/definitions and all work functions categorized as Manage, Design, Implement, or Evaluate.

2.1 Data Security

Refers to the 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.

2.1.1 Manage

- Ensure that security classification and data management policies and guidance are issued and updated
- Specify policy and coordinate review and approval
- Report compliance to data security policies
- Provide oversight
- Implement appropriate changes and improvement actions as required

2.1.2 Design

- Develop the data security policy using data security standards, guidelines, and requirements that include privacy, access, incident management, disaster recovery, and configuration
- Identify and document the appropriate level of protection for the data
- Specify information classification, sensitivity, and need-to-know requirements by data or data type
- Create data user authentication and authorization system data access levels and privileges
- 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
- Identify appropriate set of information security controls based on perceived risk of compromise to the data

2.1.3 Implement

- Perform the data access management process according to established guidelines
- Apply and maintain data security controls and processes in accordance with data security policy, guidelines, and requirements
- Apply media controls and processes
- Apply and verify data security access controls and privileges
- Address alleged violations of data security and privacy breaches

- Apply and maintain privacy controls in accordance with privacy guidance in accordance with standards, procedures, directives, policy, regulations, and laws

2.1.4 Evaluate

- Assess the effectiveness of the enterprise data security policies, processes, and procedures against established standards, guidelines, and requirements and suggest changes where appropriate
- Evaluate the effectiveness of products and technologies implemented to provide the required protection of data
- Review alleged violations of data security and privacy breaches
- Identify improvement actions required to maintain appropriate level of data protection

2.2 Digital Forensics

Refers to the knowledge and understanding of digital investigation and analysis techniques used for recovering, authenticating, and analyzing electronic data to reconstruct events related to security incidents. Such activities require building a digital knowledge base. The investigative process is composed of three phases: acquire, analyze, and report.

2.2.1 Manage

- Acquire the necessary contractual vehicle and resources, including financial resources, to run forensic labs and programs
- Coordinate and build internal and external consensus for developing and managing an organizational digital forensic program
- Establish a digital forensic team, usually composed of investigators, IT professionals, and incident handlers, to perform digital and network forensics
- Provide adequate work spaces that at a minimum take in to account electrical, thermal, acoustic, and privacy concerns (i.e., intellectual properties, classification, contraband) and security requirements (including access control) of equipment and personnel as well as provide adequate report writing/administrative areas
- Implement appropriate changes and improvement actions as required

2.2.2 Design

- Create policies and procedures for establishing and/or operating a digital forensic unit in accordance with standards, procedures, directives, policy, regulations, and law
- Establish policies for the imaging (bit for bit copying) of electronic media
- Specify hardware and software requirements to support the digital forensic program
- Establish the hardware and software requirements (configuration management) of the forensic laboratory
- Develop policies for the preservation of electronic evidence, data recovery and analysis, reporting and archival requirements of examined material in accordance with standards, procedures, directives, policy, regulations, and laws

- Consider establishing examiner requirements that include an ongoing mentorship program, competency testing prior to assuming individual case responsibilities, periodic proficiency testing, and participation in a nationally recognized certification program that encompasses a continuing education requirement
- Adopt or create a chain of custody procedures that include disposal procedures and when required, the return of media to its original owner in accordance with standards, procedures, directives, policy, regulations, and law

2.2.3 Implement

- Assist in collecting and preserving evidence in accordance with established procedures, plans, policies, and best practices
- Perform forensic analysis on networks and computer systems and make recommendations for remediation
- Apply, maintain, and analyze results from intrusion detection systems, intrusion prevention systems, network mapping software, and other tools to protect, detect, and correct information security-related vulnerabilities and events
- Follow proper chain-of-custody best practices in accordance with standards, procedures, directives, policy, regulations, and law
- Collect and retain audit data to support technical analysis relating to misuse, penetration reconstruction, or other investigations
- Provide audit data to appropriate law enforcement or other investigating agencies to include corporate security elements
- Assess and extract the relevant pieces of information from the collected data
- Report complete and accurate findings and the result of analysis of digital evidence to appropriate resources
- Coordinate dissemination of forensic analysis findings to appropriate resources
- Provide training, as appropriate, on using forensic analysis equipment, technologies, and procedures, such as the installation of forensic hardware and software components
- Acquire and manage a Standard Operating Environment (SOE) (baseline standard) of company or agency computer footprint
- Coordinate applicable legal and regulatory compliance requirements
- Coordinate, interface and work under the direction of appropriate corporate entities (e.g., corporate legal, corporate investigations) with regard to investigations or other legal requirements, including investigations that involve external governmental entities (e.g., international, national, state, local)

2.2.4 Evaluate

- Ensure the effectiveness and accuracy of forensic tools used by digital forensic examiners and implement changes as required
- Assess the effectiveness, accuracy and appropriateness of testing processes and procedures that are followed by the forensic laboratories and teams and suggest changes where appropriate

- Assess the digital forensic staff to ensure that they have the appropriate knowledge, skills, and abilities to perform forensic activities
- Validate the effectiveness of the analysis and reporting process and implement changes where appropriate
- Review and recommend standard validated forensic tools
- Assess the digital forensic laboratory quality assurance program, monitor, peer review process, audit and proficiency testing procedures and implement changes where appropriate
- Examine penetration testing and vulnerability analysis results to identify risks and implement patch management
- Identify improvement actions based on the results of validation, assessment, and review

2.3 Enterprise Continuity

Refers to the application of the principles, policies, and procedures used to ensure an enterprise continues to perform essential business functions after the occurrence of a wide range of potential catastrophic events. For the purposes of the IT Security EBK, Enterprise Continuity relates to IT assets and resources and associated IT security requirements.

2.3.1 Manage

- Coordinate with corporate stakeholders to establish the enterprise continuity of operations program
- Acquire the necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program
- Define the enterprise continuity of operations organizational structure and staffing model
- Define emergency delegations of authority and orders of succession for key positions
- Direct contingency planning, operations, and programs to manage risk
- Define the scope of the enterprise continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery and related activities
- Integrate enterprise concept of operations activities with related contingency planning activities
- Establish an enterprise continuity of operations performance measurement program
- Identify and prioritize critical business functions
- Implement appropriate changes and improvement actions as required

2.3.2 Design

- Develop strategic policy for the organization's continuity of operations
- Develop an enterprise continuity of operations plan and procedures
- Develop and maintain enterprise continuity of operations documentation such as contingency, business continuity, business recovery, disaster recovery, and incident handling plans

- Develop a comprehensive test, training, and exercise program to evaluate and validate the readiness of enterprise continuity of operations plans, procedures, and execution
- Prepare internal and external continuity of operations communications procedures and guideline

2.3.3 Implement

- Execute the enterprise continuity of operations and related contingency plans and procedures
- Control access to information assets during an incident in accordance with the organizational policy
- Execute crisis management tests, training, and exercises and apply lessons learned from them

2.3.4 Evaluate

- 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 implement changes where appropriate
- Continuously validate the organization against additional mandates, as developed, to ensure full compliance
- Collect and report performance measures and identify improvement actions

2.4 Incident Management

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

2.4.1 Manage

- Coordinate with stakeholders to establish the incident management program
- Establish relationships between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations Professionals)
- Acquire and manage the resources, including financial resources, for the incident management functions
- Ensure the coordination between the incident response team and the security administration and technical support teams
- Apply lessons learned from information security incidents to improve incident management processes and procedures
- Implement appropriate changes and improvement actions as required

2.4.2 Design

- Develop the incident management policy
- Identify the services the incident response team should provide

- Create incident response plans in accordance with security policy and organizational goals
- Develop procedures for performing incident handling and reporting
- Create incident response exercises and red teaming activities
- Develop specific processes for collecting and protecting forensic evidence during incident response
- Specify the incident response staffing and training requirements
- Establish incident management measurement program

2.4.3 Implement

- Apply response actions in reaction to security incidents in accordance with established policy, plans, and procedures
- Respond to and report incidents
- Assist in collecting, processing, and preserving evidence according to standards, procedures, directives, policy, regulations, and law
- Monitor the network and information systems for intrusions
- Execute incident response plans
- Execute red teaming activities and incidence response exercises
- Ensure lessons learned from incidents are collected in a timely manner and are incorporated into plan reviews
- Collect, analyze, and report incident management measures

2.4.4 Evaluate

- Assess the efficiency and effectiveness of the incident response program activities and implement changes as required
- Examine the effectiveness of red teaming and incident response tests, training, and exercises
- Assess the effectiveness of communications between incident response team and related internal and external organizations and implement changes where appropriate
- Identify incident management improvement actions based on assessments of effectiveness

2.5 IT Security Training and Awareness

Refers to the principles, practices, and methods required to raise employee awareness about basic information security, and to train individuals with information security roles to increase their knowledge, skills and abilities. Training activities are designed to instruct workers about their security responsibilities and teach them about information security processes and procedures so duties are performed optimally and securely within related environments. Awareness activities present essential information security concepts to the workforce in order to change user behavior.

2.5.1 Manage

- Identify business requirements and establish the enterprise-wide policy for the IT security awareness and training program

- Acquire and manage the necessary resources, including financial resources, to support the IT awareness and training program
- Set operational performance measures for training and delivery and ensure that they are met
- Ensure the organization complies with IT security awareness and training standards/requirements
- Implement appropriate improvement actions as required

2.5.2 Design

- Develop the security awareness and training policy
- Define the goals and objectives of the IT security awareness and training program
- Work with appropriate security subject-matter experts to ensure the completeness and accuracy of the security training 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

2.5.3 Implement

- Perform 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 the intended audiences
- Deliver awareness and training to the intended audiences based on identified needs
- Update awareness and training materials when necessary
- Communicate the management commitment and importance of the IT security awareness and training program to the workforce

2.5.4 Evaluate

- Assess and evaluate the IT security awareness and training program for compliance with corporate policy and measure performance of the program against objectives
- Review the IT security awareness and training program materials and recommend improvements
- Audit the awareness and training program to ensure that it meets the organization's stakeholder needs
- Ensure that information security personnel are receiving the appropriate level and type of training
- Collect, analyze, and report performance measures

2.6 IT Systems Operations and Maintenance

Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on it during the operations phase of an IT system or application in production.

2.6.1 Manage

- Establish the security administration program goals and objectives
- Monitor the security administration program budget
- Direct the security administration personnel
- Address security administration program risks
- Define the scope of the security administration program
- Establish communications between the security administration team and other security-related personnel (e.g., technical support, incident management)
- Integrate the security administration team activities with other security-related team activities (e.g., technical support, incident management, security engineering)
- Acquire the necessary resources, including financial resources, to execute the security administration program
- Ensure operational compliance with applicable legislation, regulations, standards, and policies
- Implement appropriate improvement actions, as required

2.6.2 Design

- Develop security administration processes and procedures in accordance with standards, procedures, directives, policy, regulations, and laws
- Develop personnel, application, middleware, operating system, hardware, network, facility, and egress security controls
- Develop security administration tests, test scripts, test criteria, and testing procedures
- Develop security administration change management procedures to ensure security policies and controls remain effective following a change
- Recommend appropriate forensics sensitive policies into the enterprise security plan

2.6.3 Implement

- Perform security administration processes and procedures in accordance with standards, procedures, directives, policy, regulations, and law
- Establish a secure computing environment by applying, monitoring, controlling, and managing security controls
- Ensure that information systems are assessed regularly for vulnerabilities and that appropriate solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented
- Monitor IT security performance measures to ensure optimal system performance

- Perform security performance testing and reporting and recommend security solutions in accordance with standards, procedures, directives, policy, regulations, and law
- Perform security administration changes and validation testing
- Identify, control, and track all IT security configuration items
- Collaborate with the technical support, incident management, and security engineering teams to develop, implement, control, and manage new security administration technologies
- Monitor vendor agreements and Service Level Agreement's (SLA) to ensure that contract and performance measures are achieved
- Establish and maintain controls and surveillance routines to monitor and control conformance to all applicable information security laws and regulations

2.6.4 Evaluate

- Review strategic security technologies
- Review the performance and correctness of applied security controls in accordance with standards, procedures, directives, policy, regulations, and law and apply corrections as required
- Assess the performance of security administration measurement technologies
- Assess system and network vulnerabilities
- Assess compliance with standards, procedures, directives, policy, regulations, and law
- Identify improvement actions based on reviews, assessments, and other data sources

2.7 Network Security and Telecommunications

Refers to the application of the principles, policies, and procedures involved in ensuring the security of basic network services and data and in maintaining the hardware layer on which it resides. These practices address perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.

2.7.1 Manage

- Establish a network security and telecommunications program in line with enterprise policy and security goals
- Manage the necessary resources, including financial resources, to establish and maintain an effective network security and telecommunications program
- Direct network security and telecommunications personnel
- Define the scope of the network security and telecommunications program
- Establish communications between the network security and telecommunications team and related security teams (e.g., technical support, security administration, incident response)
- Integrate network security and telecommunications program activities with technical support, security administration, and incident response activities
- Establish a network security and telecommunications performance measurement program

- Ensure enterprise compliance with applicable network-based standards, procedures, directives, policies, regulations, and laws
- Ensure that network-based audits and management reviews are conducted to implement process improvement
- Implement appropriate improvement actions, as required

2.7.2 Design

- Develop network and host-based security policies in accordance with standards, procedures, directives, policies, regulations, and laws
- Specify strategic security plans for network telecommunications in accordance with established policy to meet organizational security goals
- Develop network security and telecommunications operations and maintenance standard operating procedures
- Develop network security test plans and procedures in accordance with standards, procedures, directives, policies, regulations, and laws
- Generate network security performance reports
- Develop network security and telecommunication audit processes and procedures

2.7.3 Implement

- Prevent and detect intrusions and protect against viruses
- Perform audit tracking and reporting
- Create, develop, apply, control, and manage effective network domain security controls in accordance with enterprise, network, and host-based policies
- Test strategic network security technologies for effectiveness; incorporate controls that ensure compliance with the enterprise, network and host-based security policies
- Monitor and assess network security threats and issues
- Gather technical data and monitor and assess network vulnerabilities
- Correct network security vulnerabilities in response to problems identified in vulnerability reports
- Provide real-time network intrusion response
- Determine whether or not antivirus systems are in place and operating correctly
- Ensure that messages are confidential and free from tampering and repudiation
- Defend network communications from tampering and/or eavesdropping

2.7.4 Evaluate

- Perform a network security evaluation, calculate risks to the enterprise, and recommend remediation activities
- Ensure that appropriate solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented effectively

- Arrange independent verification and validation of the network to assess full satisfaction of functional requirements
- Compile data into measures for analysis and reporting

2.8 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. The controls include organization/functional design elements such as separation of duties, job rotation, and determining position sensitivity.

2.8.1 Manage

- Coordinate with IT security, physical security, operations security, and other organizational managers to ensure a coherent, coordinated approach to security across the organization
- Acquire and manage the necessary resources, including financial resources, to manage and maintain the personnel security program
- Establish objectives for the personnel security program relative to the overall security goals for the enterprise
- Ensure compliance through periodic audits of methods and controls
- Ensure personnel security is a component of enterprise continuity of operations
- Direct the ongoing operations of the personnel security program
- Implement appropriate improvement actions, as required

2.8.2 Design

- Establish personnel security processes and procedures for individual job roles
- Establish procedures to coordinate with other organizations to ensure common processes are aligned
- Establish personnel security standards to which external suppliers (e.g., vendors, contractors) must conform

2.8.3 Implement

- Coordinate within the personnel security office or with Human Resources to ensure that position sensitivity is established prior to the interview process and that appropriate background screening and suitability requirements are identified for each position
- Coordinate within the personnel security office or with Human Resources to ensure background investigations are processed based on the level of trust and position sensitivity
- Review, analyze, and adjudicate reports of investigations, personnel files, and other records to determine whether to grant, deny, revoke, suspend, or restrict clearances consistent with national security and/or suitability issues
- Coordinate with physical security and IT security operations personnel to ensure that employee access to physical facilities, media, and IT systems and networks is modified or terminated upon reassignment, change of duties, resignation, or termination

- Exercise oversight of personnel security program appeals procedures to verify that the rights of individuals are being protected according to law
- Periodically review the personnel security program for compliance with standards, procedures, directives, policy, regulations, and law

2.8.4 Evaluate

- Review the 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 assess the personnel security program for compliance with standards, procedures, directives, policies, regulations, and laws

2.9 Physical and Environmental Security

Refers to the methods and controls used to proactively protect an organization from natural or manmade 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 information.

2.9.1 Manage

- Coordinate with personnel managing IT security, personnel security, operations security, and other security program areas to provide an integrated and coherent security effort
- Acquire the necessary resources, including financial resources, to support an effective physical security program
- Establish a physical security performance measurement system
- Establish a program to determine the value of physical assets and their impact if unavailable
- Implement appropriate improvement recommendations, as required

2.9.2 Design

- Identify the physical security program requirements and specifications in relationship to the enterprise security goals
- Develop the 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

2.9.3 Implement

- Apply physical and environmental controls in support of the physical security plan

- Control access to information assets in accordance with standards, procedures, directives, policy, regulations, and law
- Integrate physical security concepts into test plans, procedures, and exercises
- Conduct threat and vulnerability assessments to identify physical and environmental risks and vulnerabilities then update the applicable controls as necessary
- Review construction projects to ensure that appropriate physical security and protective design features are incorporated into the design

2.9.4 Evaluate

- Assess and evaluate the overall effectiveness of the physical and environmental security policy and controls and make recommendations for improvement
- Review incident data and make process improvement recommendations
- Assess the effectiveness of physical and environmental security control testing
- Evaluate acquisitions that have physical security implications and report findings to management
- Compile, analyze, and report performance measures

2.10 Procurement

Refers to the application of principles, policies, and procedures required to plan, apply, and evaluate the purchase of IT products or services, including "risk-based" pre-solicitation, solicitation, source selection, award, and monitoring, disposal, and other post-award activities. Procurement activities may consist of the development of procurement and contract administration documents that include, but are not limited to, procurement plans, estimates, requests for information, requests for quotes, requests for proposals, statements of work, contracts, cost-benefit analyses, evaluation factors for award, source selection plans, incentive plans, service level agreements, justifications required by policies or procedures, and contract administration plans.

2.10.1 Manage

- Collaborate with various stakeholders (which may include internal client, lawyers, Chief Information Officer (CIO), Chief Information Security Officer, IT Security Professional, Privacy Professional, Security Engineer, suppliers, and many others) on the procurement of IT security products and services
- Ensure the inclusion of risk-based IT security requirements in acquisition plans, cost estimates, statements of work, contracts, and evaluation factors for award, service level agreements, and other pertinent procurement documents
- Ensure that suppliers understand the importance of IT security
- Conduct detailed IT investment reviews and security analyses and review IT investment business cases for security requirements
- Ensure that organization's IT contracts do not violate laws and regulations, and require compliance with standards when applicable
- Specify policies for the use of third party information by vendors/partners and connection requirements and acceptable use policies for vendors that connect to networks

- Implement appropriate improvement recommendations, if required

2.10.2 Design

- Develop contracting language that mandates the incorporation of IT security requirements in information services, IT integration services, IT products, and information security product purchases
- Develop contract administration policies that direct the evaluation and acceptance of delivered IT security products and services under a contract, as well as the security evaluation of IT and software being procured
- Develop measures and reporting standards to measure and report on key objectives in procurements aligned with IT security policies and procedures
- Develop a vendor management policy and associated program that implements policy with regard to use of third party information and connection requirement and acceptable use policies for vendors who connect to corporate networks. Include due diligence activities to ensure that vendors are operationally and technically competent to receive third party information and to connect and communicate with corporate networks

2.10.3 Implement

- Include IT security considerations as directed by policies and procedures in procurement and acquisition activities
- Negotiate final deals (e.g., contracts, contract changes, grants, agreements) that include IT security requirements that minimize risk to the organization
- Ensure that physical security concerns are integrated into the acquisition strategies
- Maintain ongoing and effective communications with suppliers and providers
- Perform compliance reviews of delivered products and services to assess the delivery of IT requirements against stated contract requirements and measures

2.10.4 Evaluate

- Review contracting documents, such as statements of work or requests for proposals, for inclusion of IT security considerations in accordance with information security requirements, policies, and procedures
- Assess industry landscape for applicable IT security trends, including practices for mitigating security risks associated with global supply chain management
- Review Memorandum of Agreements, Memorandum of Understandings and/or Service Level Agreements for agreed level of IT security responsibility
- Conduct detailed IT investment reviews and security analyses and review IT investment business cases for security requirements
- Assess and evaluate the effectiveness of the vendor management program in complying with corporate policy with regard to use of third party information and connection requirement and acceptable use policies for vendors who connect to corporate networks
- Conduct due diligence activities to ensure that vendors are operationally and technically competent to receive third party information, to connect and communicate with networks, and to deliver and support secure applications

- Evaluate effectiveness of procurement function at addressing information security requirements through procurement activities and recommend improvements

2.11 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.

2.11.1 Manage

- Establish and administer a risk-based enterprise information security program that addresses applicable standards, procedures, directives, policies, regulations and laws
- Define the scope of the enterprise information security compliance program
- Maintain the information security enterprise compliance program budget
- Organize and direct a staff that is responsible for information security compliance, licensing and registration, and data security surveillance
- Ensure that all employees are informed of their obligations and are motivated to comply with the applicable information security standards, procedures, directives, policies, regulations, and laws
- Identify major enterprise risk factors (product, compliance, and operational) and develop and coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk
- Maintain relationships with all regulatory information security organizations and appropriate industry groups, forums, stakeholders and organizations
- Keep informed on pending information security changes, trends, and best practices by participating in collaborative settings
- Secure the resources necessary to support an effective information security enterprise compliance program
- Establish an enterprise information security compliance performance measures program
- Implement appropriate improvements, as required

2.11.2 Design

- Develop enterprise information security compliance strategies, policies, plans, and procedures in accordance with established standards, procedures, directives, policies, regulations, and laws
- Specify enterprise information security compliance program control requirements
- Author information security compliance performance reports
- Document information security audit results and develop remedial action policies and procedures
- Develop a plan of action and associated mitigation strategies to address program deficiencies

- Document compliance reporting process in a manner that produces evidence that process exists

2.11.3 Implement

- Monitor and assess the information security compliance practices of all personnel in accordance with enterprise policies and procedures
- Maintain ongoing and effective communications with key compliance stakeholders
- Conduct internal audits to determine if information security control objectives, controls, processes, and procedures are effectively applied and maintained, and perform as expected

2.11.4 Evaluate

- Assess the effectiveness of enterprise compliance program controls against the applicable laws, regulations, standards, policies, and procedures
- Assess the effectiveness of the information security compliance process and procedures for process improvement and implement changes where appropriate
- Compile, analyze, and report performance measures

2.12 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 and to manage mitigation strategies that achieve the security needed at an affordable cost.

2.12.1 Manage

- Establish a IT security risk management program based on the enterprise business goals and objectives
- Advise senior management during the decision making process by helping them understand and evaluate the impact of IT security risks on business goals, objectives, plans, programs and actions
- Acquire and manage the resources, including financial resources, necessary to conduct an effective risk management program
- Authorize operations to acknowledge acceptance of residual risk
- Implement appropriate improvement recommendations, as required

2.12.2 Design

- Specify risk-based information security requirements and a security concept of operations
- Develop the 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 the 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, policy, regulation, and law

2.12.3 Implement

- 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 the benefits provided by mitigating controls
- Implement threat and vulnerability assessments to identify security risks and update the applicable security controls regularly
- Identify risk/functionality tradeoffs and work with stakeholders to ensure risk management implementation is consistent with desired organization's risk posture

2.12.4 Evaluate

- Assess the effectiveness of the risk management program and implement changes where required
- Review the performance of and provide recommendations for risk management (security controls, policies/procedures that make up risk management program) tools and techniques
- Assess the residual risk in the information infrastructure used by the organization
- Assess the results of threat and vulnerability assessments to identify security risks and update the applicable security controls regularly
- Identify changes to risk management policies and processes to remain current with emerging risk and threat environment

2.13 Strategic Management

Refers to the principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. Strategic management requires the practice of external business analyses such as customer analyses, competitor analyses, market analyses, and industry environmental analyses. Strategic management also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities and constraints. The goal of these analyses is to ensure that an organization's IT security principles, practices and system design are in line with the organization's mission statement.

2.13.1 Manage

- Establish an IT security program to provide security for all systems, networks, and data that support the operations and business/mission needs of the organization
- Integrate and align IT security, physical security, personnel security, and other security components into a systematic process to ensure information protection goals and objectives are reached
- Align IT security priorities with the organization's mission and vision and communicate the value of IT security within the organization
- Acquire the necessary resources, including financial resources, to support IT security goals and objectives and reduce overall organizational risk

- Establish overall enterprise security architecture (EA) by aligning business processes, IT software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy
- Acquire and manage the necessary resources, including financial resources, for instituting the security policy elements in the operational environment
- Establish the organizational goals that are in accordance with standards, procedures, directives, policies, regulations and laws
- Balance the IT security investment portfolio based on EA considerations and enterprise security priorities

2.13.2 Design

- Establish a performance management program that will measure the efficiency, effectiveness, and maturity of the IT security program in support of the business/mission needs of the organization
- Develop IT security program components and associated strategy to support organization's IT security program
- Develop information security management strategic plans
- Integrate applicable laws and regulations into the enterprise information security strategy, plans, policies, and procedures

2.13.3 Implement

- Provide feedback to management on the effectiveness and performance of security strategic plans in accomplishing business/mission needs
- Perform internal and external enterprise analyses to ensure the organization's IT security principles and practices are in line with the organizational mission
- Integrate business goals with information security program policies, plans, processes, and procedures
- Collect, analyze, and report performance measures
- Use performance measures to inform strategic decision making

2.13.4 Evaluate

- Determine if security controls and processes are adequately integrated into the investment planning process based on IT portfolio and security reporting
- Review security funding within IT portfolio to determine if funding accurately aligns with security goals and objectives and make funding recommendations accordingly
- Assess the integration of security with the business/mission and recommend improvements
- Review the cost goals of each major investment
- Assess the performance and overall effectiveness of the security program with respect to security goals and objectives
- Assess and refresh performance measurement program to ensure currency with organization's goals and priorities

2.14 System and Application Security

Refers to the principles, policies, and procedures pertaining to integrating information security into an IT system or application during the System Development Life Cycle (SDLC) prior to the Operations and Maintenance phase. The practice of these protocols ensures that the operation of IT systems and software does not present undue risk to the enterprise and its information assets. This objective is accomplished through risk assessment; risk mitigation; security control selection, implementation and evaluation; and software security standards compliance.

2.14.1 Manage

- Establish the IT system and application security engineering program
- Acquire the necessary resources, including financial resources, to support the integration of security in the SDLC
- Guide IT security personnel through the SDLC phases
- Define the scope of the IT security program as it applies to the application of SDLC
- Plan the IT security program components into the SDLC

2.14.2 Design

- Specify the enterprise and IT system or application security policies
- Specify the security requirements for the IT system or application
- Author an IT system or application security plan in accordance with the enterprise and IT system or application security policies
- Identify the standards against which to engineer the IT system or application
- Specify the criteria for performing risk-based audits against the IT system or application
- Develop processes and procedures to mitigate the introduction of vulnerabilities during the engineering process
- Integrate applicable information security requirements, controls, processes, and procedures into IT system and application design specifications in accordance with established standards, policies, regulations, and laws

2.14.3 Implement

- Execute the enterprise and IT system or application security policies
- Apply and verify compliance with the identified standards against which to engineer the IT system or application
- Perform the processes and procedures to mitigate the introduction of vulnerabilities during the engineering process
- Perform secure configuration management practices
- Validate that the engineered IT security and application security controls meet the specified requirements
- Reengineer security controls to mitigate vulnerabilities identified during the operations phase
- Ensure the integration of information security practices throughout the SDLC process

- Document IT or application security controls addressed within the system
- Practice secure coding practices

2.14.4 Evaluate

- Review new and existing risk management technologies to achieve an optimal enterprise risk posture
- Review new and existing IT security technologies to support secure engineering across the SDLC phases
- Continually assess the effectiveness of the information system's controls based on risk management practices and procedures
- Assess and evaluate system compliance with corporate policies and architectures
- Assess system maturation and readiness for promotion to the production stage
- Collect lessons learned from integration of information security into the SDLC and use to identify improvement actions
- Collect, analyze, and report performance measures

3 The IT Security Essential Body of Knowledge

Knowledge of key terms and concepts is the foundation for effective performance of the functions associated with each of the technical competency areas. Without requisite knowledge, it is virtually impossible to perform work functions.

The IT Security EBK lists all of the key terms and concepts that have been identified for each competency area. At minimum, individuals should know, understand, and be able to apply the key terms and concepts that relate to the competencies to which their role is linked. Full knowledge of all of the key terms and concepts is the foundation for performance as a conversant IT security generalist. This section describes and lists the 14 IT security competency areas with affiliated key terms and concepts.

3.1 Data Security

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

- Access Control
- Aggregation
- Antivirus Software
- Authentication
- Data Classification
- Discretionary Access Control
- Encryption
- Electronic Commerce
- Firewall Configuration
- Information Classification Scheme
- Mandatory Access Control
- Need-To-Know
- Nonrepudiation
- Personally Identifiable Information
- Privacy
- Privilege Levels
- Public Key Infrastructure
- Role-Based Access Control
- Rule-Based Access Control
- Secure Data Handling
- Security Clearance
- Sensitive Information
- Sensitivity Determination
- Sensitivity of Data
- Steganography
- System of Records
- User Privileges
- User Provisioning

986

3.2 Digital Forensics

Refers to the knowledge and understanding of digital investigation and analysis techniques used for recovering, authenticating, and analyzing electronic data to reconstruct events related to security incidents. Such activities require building a digital knowledge base. The investigative process is composed of three phases: acquire, analyze, and report.

- Bit-Stream Copy/Image
- Chain of Custody
- Cluster
- Computer Forensics
- Copy/Image
- Cyber Laws/Guidelines/Policies
- Digital Forensic Systems
- Disk File System
- Duplicate Image
- Evidence Archival
- Forensic Analysis
- Forensic Labs
- Integrity of Evidence
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Network Forensics
- Network Monitoring
- Persistent Data
- Portable Media Forensics
- Security Incident

987
988

3.3 Enterprise Continuity

Refers to the application of the principles, policies, and procedures used to ensure an enterprise continues to perform essential business functions after the occurrence of a wide range of potential catastrophic events. For the purposes of the IT Security EBK, Enterprise Continuity relates to IT assets and resources and associated IT security requirements.

- Alternate Facility
- Business Continuity
- Business Recovery
- Crisis Communication
- Cyber Incident Response
- Delegation of Authority
- Disaster Recovery
- Disruption
- Essential Functions
- Information Technology Contingency Plan
- Interoperable Communications
- Occupant Emergency
- Order of Succession
- Preparedness/Readiness
- Risk Mitigation
- Standard Operating Procedures
- Tests, Training, and Exercises
- Threat Environment
- Vital Records and Databases

989

990

3.4 Incident Management

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

- Computer Security
- Escalation Procedures
- Incident Handling
- Incident Records
- Incident Response
- Information Assurance Posture
- Information Security Policy
- Information System
- Intrusion
- Measures
- Privacy (personally identifiable data)
- Reconstitution of System
- Risk
- Risk Assessment
- Risk Management
- Security Alerts
- Security Incident
- System Compromise
- Threat
- Threat Motivation
- Unauthorized Access
- User
- Vulnerability

991
992

3.5 IT Security Training and Awareness

Refers to the principles, practices, and methods required to raise employee awareness about basic information security, and to train individuals with information security roles to increase their knowledge, skills and abilities. Training activities are designed to instruct workers about their security responsibilities and teach them about information security processes and procedures so duties are performed optimally and securely within related environments. Awareness activities present essential information security concepts to the workforce in order to change user behavior.

- Awareness
- End User Security Training
- IT Security Awareness Program
- Instructor Led Training (ILT)
- Computer Based Training (CBT)
- Curriculum
- Learning Objectives
- IT Security Training Program
- Role-Based Training
- Training
- Instructional Systems Design (ISD)
- Web Based Training (WBT)
- Learning Management System (LMS)
- Needs Assessment

993

994

3.6 IT Systems Operations and Maintenance	
Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on it during the operations phase of an IT system or application in production.	
• Access Control • Antivirus Software • Backups • Configuration Management • Insider Threat • Intrusion Detection Systems • Intrusion Prevention Systems • Patch Management • Penetration Testing	• Security Data Analysis • Security Measures • Security Reporting • System Hardening • System Logs • System Monitoring • Threat Analysis • Threat Monitoring • Vulnerability Analysis

995
996

3.7 Network Security and Telecommunications	
Refers to the application of the principles, policies, and procedures involved in ensuring the security of basic network services and data and in maintaining the hardware layer on which it resides. These practices address perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.	
• Access Control • Biometrics Authentication • Configuration • Cryptosecurity • Defense-in-Depth • Email Scanners • Emission Security • Encryption Technologies (e.g., Secure Sockets Layer [SSL], Transport Layer Security [TLS]) • Firewalls • Hubs • Internal and External Telecommunications Technology (e.g., Private Branch Exchange [PBX] and Voice Over Internet Protocol [VOIP]) • Intrusion Detection Systems	• Intrusion Prevention Systems • Load Balancers • Network Architecture • Network Segmentation (e.g., Virtual Local Area Network [V-LAN], Demilitarized Zone [DMZ]) • Penetration Testing • Port • Routers • Switches • Threat • Transmission Security • Virtual Private Network • Vulnerability

997

3.8 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. The controls include organization/functional design elements such as separation of duties, job rotation, and determining position sensitivity.

- Background Checks/Background Investigation
- Confidentiality
- Human Resources
- Insider Threat
- Job Rotation
- Nondisclosure Agreement
- Position Sensitivity
- SBI
- Secure Employee Termination Procedures
- Security Breach
- Security Clearance
- Separation of Duties

998
999

3.9 Physical and Environmental Security

Refers to the methods and controls used to proactively protect an organization from natural or manmade 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 information.

- Access Cards
- Access Control
- Biometrics
- Defense-in-Depth
- Environmental Threat
- Identification and Authentication
- Inventory
- Manmade Threat
- Natural Threat
- Perimeter Defense
- Risk Management
- Terrorism
- Threat and Vulnerability Assessment

1000

1001

3.10 Procurement

Refers to the application of principles, policies, and procedures required to plan, apply, and evaluate the purchase of IT products or services, including "risk-based" pre-solicitation, solicitation, source selection, award, and monitoring, disposal, and other post-award activities. Procurement activities may consist of the development of procurement and contract administration documents that include, but are not limited to, procurement plans, estimates, requests for information, requests for quotes, requests for proposals, statements of work, contracts, cost-benefit analyses, evaluation factors for award, source selection plans, incentive plans, service level agreements, justifications required by policies or procedures, and contract administration plans.

- Acceptable risk
- Acquisition
- Acquisition Life Cycle
- Award
- Benchmarking
- Business Impact
- Category Management
- Contract
- Cost-Benefit Analysis
- Cost Reimbursement Contract
- eSourcing
- Estimation
- Fixed Price Contract
- Incentive Contract
- Indefinite Delivery Contract
- Performance-based Contracts
- Prequalification
- Regulatory Compliance
- Request for Information
- Request for Proposal
- Risk Analysis
- Risk-Based Decision
- Risk Mitigation
- Security
- Security Measures
- Service Level Agreement
- Solicitation
- Sole Source Justification
- Spend Analysis
- Statement of Objectives
- Statement of Work
- Terms and Conditions
- Time and Materials Contract
- Total Cost of Ownership

1002

1003

3.11 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.

- Assessment
- Auditing
- Certification
- Compliance
- Ethics
- Evaluation
- Governance
- Laws (including but not limited to Health Insurance Portability and Accountability Act [HIPAA], Federal Information Security Management Act [FISMA], Clinger-Cohen Act, Privacy Act, Sarbanes-Oxley, etc.)
- Policy
- Privacy Principles/Fair Info Practices
- Procedure
- Regulations
- Security program
- Standards (e.g., ISO 27000 series, Federal Information Processing Standards [FIPS])
- Validation
- Verification

1004
1005

3.12 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 and to manage mitigation strategies that achieve the security needed at an affordable cost.

- Acceptable Risk
- Annual Loss Expectancy
- Annual Rate of Occurrence
- Asset Valuation
- Benchmarking
- Business Impact
- Likelihood Estimation
- Management
- Risk Analysis
- Risk Mitigation
- Risk Treatment
- Security
- Security Measures
- Single Loss Expectancy
- Threat
- Threat and Vulnerability Assessment
- Threat Modeling
- Types of Risk
- Vulnerability

1006
1007

3.13 Strategic Management

Refers to the principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. Strategic management requires the practice of external business analyses such as customer analyses, competitor analyses, market analyses, and industry environmental analyses. Strategic management also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities and constraints. The goal of these analyses is to ensure that an organization's IT security principles, practices and system design are in line with the organization's mission statement.

- Acquisition Management
- Budgeting Process and Financial Management
- Built-In Security
- Capital Planning
- Enterprise Architecture
- Enterprise Security
- Performance Management
- Strategic Planning
- Strategic Resource and Investment Management

1008
1009

3.14 System and Application Security

Refers to the principles, policies, and procedures pertaining to integrating information security into an IT system or application during the SDLC prior to the Operations and Maintenance phase. The practice of these protocols ensures that the operation of IT systems and software does not present undue risk to the enterprise and its information assets. This objective is accomplished through risk assessment; risk mitigation; security control selection, implementation and evaluation; and software security standards compliance.

- Accreditation
- Application and Technical Security Controls
- Application Development
- Certification
- Configuration Management
- Process Maturity
- Risk Mitigation
- Secure Coding
- Security Management
- Security Testing and Evaluation
- System Development Life Cycle
- Risk Assessment
- Secure System Design
- Security Requirements Analysis
- Security Specifications
- Software Assurance
- System Engineering

4 IT Security Roles, Competencies and Functional Perspectives

Ten roles have been identified to segment the multitude of job titles within the public and private sector workforce into manageable functional groupings. Each role represents a cluster of organizational positions/job titles that perform similar functions in the workplace and therefore have the same IT security competencies.

4.1 Chief Information Officer

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

Competencies:

- Data Security: *Manage*
- Enterprise Continuity: *Manage*
- Incident Management: *Manage*
- IT Security Training and Awareness: *Manage*
- Physical and Environmental Security: *Manage*
- Procurement: *Manage, Design*
- Regulatory and Standards Compliance: *Manage, Evaluate*
- Risk Management: *Manage, Evaluate*
- Strategic Management: *Manage, Design, Evaluate*
- System and Application Security: *Manage*

Example Job Titles:

- Chief Information Officer (CIO)

4.2 Digital Forensics Professional

The Digital Forensics Professional performs a variety of highly technical analyses and procedures in collecting, processing, preserving, analyzing, and presenting computer-related evidence, including but not limited to data retrieval, breaking passwords, and finding hidden or otherwise "invisible" information.

Competencies:

- Digital Forensics: *Manage, Design, Implement, Evaluate*
- Incident Management: *Implement*
- IT Systems Operations and Maintenance: *Design, Implement, Evaluate*
- Network Security and Telecommunications: *Design, Implement*
- Procurement: *Evaluate*
- Risk Management: *Implement*

Example Job Titles:

- Digital Forensics Analyst

- Digital Forensics Engineer
- Digital Forensics Practitioner
- Digital Forensics Professional

4.3 Information Security Officer/Chief Security Officer

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

Competencies:

- Data Security: *Manage, Design, Evaluate*
- Digital Forensics: *Manage, Design*
- Enterprise Continuity: *Manage, Evaluate*
- Incident Management: *Manage, Design, Evaluate*
- IT Security Training and Awareness: *Manage, Evaluate*
- Physical and Environmental Security: *Manage, Evaluate*
- Procurement: *Manage, Design, Evaluate*
- Regulatory and Standards Compliance: *Manage, Design, Evaluate*
- Risk Management: *Manage, Design, Evaluate*
- Strategic Management: Manage, Design, *Implement, Evaluate*
- System and Application Security: *Manage, Evaluate*

Example Job Titles:

- Chief Cyber Security Officer
- Chief Security Officer
- Information Security Officer
- Senior Agency Information Security Officer

4.4 IT Security Compliance Professional

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:

- Data Security: *Evaluate*
- Digital Forensics: *Evaluate*
- Enterprise Continuity: *Evaluate*
- Incident Management: *Evaluate*
- IT Security Training and Awareness: *Evaluate*

- IT Systems Operations and Maintenance: *Evaluate*
- Network Security and Telecommunications: *Evaluate*
- Personnel Security: *Evaluate*
- Physical and Environmental Security: *Evaluate*
- Procurement: *Evaluate*
- Regulatory and Standards Compliance: *Design, Implement, Evaluate*
- Risk Management: *Implement, Evaluate*
- Strategic Management: *Evaluate*
- System and Application Security: *Evaluate*

Example Job Titles:

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

4.5 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.

Competencies:

- Data Security: *Design*, *Evaluate*
- IT Operations and Maintenance: *Design, Implement*
- Network Security and Telecommunications: *Design, Implement*
- Risk Management: *Implement*
- System and Application Security: *Design, Implement, Evaluate*

Example Job Titles:

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

4.6 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.

Competencies:

- Data Security: *Implement, Evaluate*
- Digital Forensics: *Implement*

- Enterprise Continuity: *Design, Implement*
- Incident Management: *Design, Implement, Evaluate*
- IT Systems Operations and Maintenance: *Manage, Design, Implement, Evaluate*
- Network Security and Telecommunications: *Manage, Design, Implement, Evaluate*
- Procurement: *Evaluate*
- Risk Management: *Implement*
- System and Application Security: *Implement*

Example Job Titles:

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

4.7 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.

Competencies:

- Data Security: *Manage, Design, Evaluate*
- Enterprise Continuity: *Evaluate*
- Incident Management: *Design, Evaluate*
- IT Security Training and Awareness: *Design, Implement, Evaluate*
- Personnel Security: *Design, Evaluate*
- Physical and Environmental Security: *Design, Evaluate*
- Regulatory and Standards Compliance: *Implement*
- Risk Management: Design, Implement, *Evaluate*

Example Job Titles:

- ISO
- Information Security Program Manager
- Information Systems Security Manager (ISSM)
- Information Systems Security Officer (ISSO)
- Security Program Director

4.8 Physical Security Professional

The Physical Security Professional protects physical computer systems and related buildings and equipment from intrusion and from fire and other natural and environmental hazards.

Competencies:

- Enterprise Continuity: *Design, Implement*

- Incident Management*: Implement*
- Personnel Security: *Evaluate*
- Physical and Environmental Security: *Manage, Design, Implement, Evaluate*
- Procurement: *Evaluation*
- Risk Management: *Implement*

Example Job Titles:

- Physical Security Administrator
- Physical Security Officer

4.9 Privacy Professional

The Privacy Professional is responsible for developing and managing an organization's privacy compliance program. The privacy professional establishes a risk management framework and governance model to assure the appropriate handling of Personally Identifiable Information (PII). The privacy professional ensures PII is managed throughout the information life cycle, from collection to disposal.

Competencies:

- Data Security: *Design, Evaluate*
- Incident Management: *Manage, Design, Implement, Evaluate*
- IT Security Training and Awareness: *Design, Evaluate*
- Personnel Security: *Design*, *Implement*
- Regulatory and Standards Compliance: *Manage, Design, Implement, Evaluate*
- Risk Management: *Manage, Design, Implement, Evaluate*

Example Job Titles:

- Chief Privacy Officer
- Privacy Act Officer
- Privacy Information Professional
- Privacy Officer
- Senior Agency Official for Privacy

4.10 Procurement Professional

The Procurement Professional purchases or negotiates for products (software, hardware, etc.) and services (contractor support, etc.) in support of an organization's IT strategy. In the IT security context, procurement professionals must ensure that security requirements are specified within solicitation and contract documents and ensure that only products and services meeting requirements are procured. The Procurement Professional must be knowledgeable about their industry and own organization, and must be able to effectively communicate with suppliers and negotiate terms of service.

Competencies:

- Procurement: *Manage, Design, Implement, Evaluate*

Example Job Titles:

- Acquisition Manager

1201 • Buyer
1202 • Contracting Officer
1203 • Contracting Officer's Technical Representative (COTR)
1204 • Contract Specialist
1205 • Purchasing Manager
1206

5 IT Security Role, Competency, and Functional Matrix

The IT Security Role, Competency, and Functional Matrix provides a visual representation of the linkage between roles, competency areas, and functions. In this section, the IT Security Roles are broadly grouped into Executive, Functional and Corollary categories.

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

Figure 5-1: IT Security Role, Competency and Functional Matrix

6 Appendix: List of Acronyms

Acronym	Definition
A	
A/R	Actions/Recommendations
C	
CBT	Computer Based Training
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
COBIT	Control Objectives for Information and related Technology
COTR	Contracting Officer's Technical Representative
CSO	Chief Security Officer
CWF	Critical Work Function
D	
DHS	Department of Homeland Security
DHS-NCSD	Department of Homeland Security National Cyber Security Division
DIAP	Defense-wide Information Assurance Program
DMZ	Demilitarized Zone
DoD	Department of Defense
E	
EA	Enterprise Architecture
EBK	Essential Body of Knowledge
F	
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
H	
HIPA	Health Insurance Portability and Accountability Act
I	
IA	Information Assurance
IASS	Information Assurance Skill Standard
ILT	Instructor Led Training

Acronym	Definition
ISD	Instructional Systems Design
ISO	International Standards Organization
ISO	Information Security Officer
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITSC-WG	Information Technology Security Certification Working Group
L	
LMS	Learning Management System
N	
NCSD	National Cyber Security Division
NIST	National Institute of Standards and Technology
P	
PBX	Private Branch Exchange
PCIPB	President's Critical Infrastructure Protection Board
PII	Personally Identifiable Information
S	
SDLC	System Development Life Cycle
SOE	Standard Operating Environment
SSE CMM	Systems Security Engineering Capability Maturity Model
SSL	Secure Sockets Layer
T	
T/E	Training and Education (Program)
TLS	Transport Layer Security
V	
V-LAN	Virtual Local Area Network
VOIP	Voice Over Internet Protocol
W	
WBT	Web Based Training