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

A Competency and Functional Framework for IT Security Workforce Development

Office of Cybersecurity and Communications
National Cyber Security Division

September 2008

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

Table of Contents

Figures Listing

Record of Changes Table

Version	Date	Description
May 2007	Working Draft v_0.5	Role-based Focus Group Feedback
July 2007	Draft v_1.0	NCSD Revision Cycles
Oct 2007	Draft v_1.1	Federal Register Public Notice
March 2008	Draft v_1.2	Federal Register Feedback Reflected
May 2008	Draft v_1.3	Revised Draft
September 2008	Final v_1.3	Final Release

1 Introduction

1.1 Overview

Over the past several decades, rapid evolution of technology has hastened society's transformation to a digital culture. The speed of this change has led to disparities in the composition of the information technology (IT) security workforce. Variations in training, expertise, and experience are the natural consequences of this evolution, and are reflected in the abundance of recruiting, education, and retention practices among employers. From the beginning of the digital revolution, public, private, and academic organizations have all dedicated resources to developing the IT security field of practice—and have made significant progress.

It is increasingly important for IT security professionals to meet today's challenges, and to proactively address those of the future. The openness and quantity of the systems connected to the Internet; the convergence of image, 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. The shared infrastructures, services, and information between government and industry demonstrate the need for an innovative model of the roles, responsibilities, and competencies required for an IT security workforce.

To assist organizations and current and future members of this workforce, the Department of Homeland Security National Cyber Security Division (DHS-NCSD) worked with experts from academia, government, and the private sector to develop a high-level framework that establishes a national baseline representing the essential knowledge and skills 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 the following:

- Articulating the functions that professionals within the IT security workforce perform, in a format and language that is context-neutral
- Providing content 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* builds directly upon the work of established references and best practices from both 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 generic security roles; defines four primary functional perspectives; and establishes an IT Security Role, Competency, and Functional Matrix (see Section 5). The EBK effort was launched to advance the IT security training and certification landscape and to help ensure 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 2001 to recommend policies and coordinate programs for protecting information systems for critical infrastructure—such as electrical grids 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.

Recognizing that IT security workforce development was an issue that required a focused strategy, the PCIPB created the IT Security Certification Working Group (ITSC-WG). This group was tasked with examining 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," and 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." Also in 2003, DHS-NCSD was established to act as a national focal point for cyber security including facilitating implementation of the *National Strategy* and coordinating cyber security efforts across the Nation.

A key recommendation from the work of the PCIPB's ITSC-WG serves 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 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 Department of Defense (DoD), academia, and private sector leaders in the IT and information security fields to conclude that while many worthwhile, well-regarded IT security certifications exist, they were developed in accordance with criteria based on the focus of each certifying organization and its market niche. IT professionals have a large and diverse selection of certifications to choose from to advance their careers—some are vendor-specific and highly technical, while others are broader, less technical, and vendor-neutral. For the defense sector, DoD 8570.01-M, the DoD *Information Assurance Workforce Improvement Program*, provides the basis for an enterprise-wide solution to train, certify, and manage the DoD Information Assurance (IA) workforce.

It is a challenge to identify with certainty the certifications that validate specific workforce competencies, and those that are the best choice to confirm or build the strengths of individuals serving in IT security roles. Resolving these concerns has been the goal of the T/E Program's certification-related work. In 2006, as a result of this complexity and uncertainty, 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 links competency areas and functions to general IT security roles regardless of sector. The EBK framework provides the following outcomes:

- Articulates 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 for comparing the content of IT security certifications, which have been developed independently according to varying criteria
- Promotes uniform competencies to increase the overall efficiency of IT security education, training, and professional development
- Offers a way to further substantiate the wide acceptance of existing certifications so that they can be leveraged appropriately as credentials
- Provides content that can be used to facilitate cost-effective professional development of the IT security workforce, including skills training, academic curricula, and other affiliated human resource activities.

1.4 Scope

Because DHS-NCSD provides the *IT Security EBK* for use across the public and private sectors, topics that are not applicable to these areas have not been included in this version. For example, the certification and accreditation (C&A) process, which is mandated by the Office of Management and Budget (OMB) Circular A-130 and applies only to systems that house Federal data, has not been included as a key term, concept, or function within a competency. The absence of C&A from the EBK is not meant to diminish its importance to IT security practitioners within the public sector—it is still a key term, but has not been included here because of its limited applicability across academia and private sector. The EBK will continue to be revised approximately every two years with input from subject matter experts (SME), to ensure that it remains a useful and up-to-date resource for the community.

Development of the competency and functional framework was an iterative process that involved close collaboration with SMEs from academia, industry, and government. Figure 1-1 identifies the process followed in preparing the framework. Each step is outlined below, followed by a description of the *IT Security EBK* review cycle.

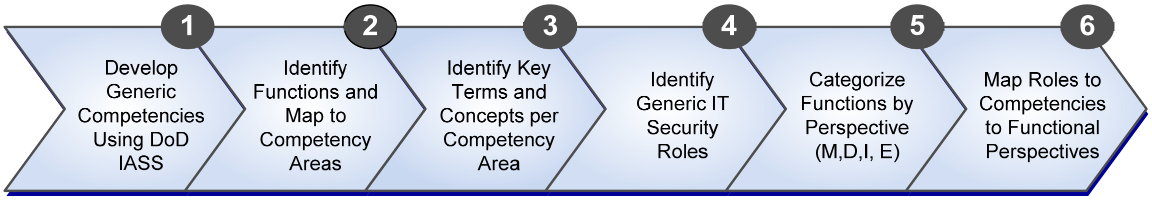

1
Develop Generic Competencies Using DoD IASS
2
Identify Functions and Map to Competency Areas
3
Identify Key Terms and Concepts per Competency Area
4
Identify Generic IT Security Roles
5
Categorize Functions by Perspective (M,D,I, E)
6
Map Roles to Competencies to Functional Perspectives

Figure 1-1: Competency and Functional Framework Development Process

Step 1: Develop Generic Competencies Using DoD Information Assurance Skill Standard (IASS). A core document that was used to shape the competency areas and functions articulated in the *IT Security EBK*, the DoD IASS was developed by the Defense-wide Information Assurance Program (DIAP) as part of the DoD 8570.01-M. DHS-NCSD participated in working groups conducted by DoD in their effort to cull 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*—i.e., "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 information assurance (IA) work within DoD according to 53 critical work functions (CWF), each of which contains multiple tasks. To begin creating a framework from which DHS-NCSD could work, the DoD IASS document was reverse-engineered to obtain the set of technical competency areas to which these 53 CWFs and tasks aligned. Each area was given a functional statement/definition to clarify the boundaries of what it would include.

Step 2: Identify Functions and Map to Competency Areas. Once competency areas were developed, the CWFs defined in the DoD IASS were mapped to them. A multitude of IT security documents were also analyzed to identify the functions associated with each area. These documents included National Institute of Standards and Technology (NIST) standards, the Committee on National Security Systems (CNSS) role-based training standards, and International Organization for Standardization (ISO) standards, as well as widely used private sector models such as Control Objectives for Information and related Technology (COBIT) and the Systems Security Engineering Capability Maturity Model (SSE CMM). Data was captured as functions rather than job tasks to allow the terminology and procedural specificity of the sector from which the data was gathered to be replaced by more general language that would apply to all sectors. It is important to note that a function was not included for the continued professional training and education of IT security professionals within each respective competency area. Emphasis of the *IT Security EBK* is on the functions themselves—it is understood that training and educational opportunities should be pursued that contribute to an IT security professional's knowledge of a competency area.

Step 3: Identify Key Terms and Concepts per Competency Area. This development step entailed identifying key terms and concepts that represent the knowledge required to perform the functions within each competency area. Key terms and concepts from all of the competency areas make up the "essential body of knowledge" for IT security (see Section 3) that is needed by a generalist in the IT security field. Because the scope of professional responsibility of practitioners performing IT security functions varies widely, knowledge of key terms and concepts is fundamental to performance. At minimum, individuals should know the key terms and concepts that correspond with the competencies mapped to their role (see Step 4 below). In most cases a key term or concept was assigned to only one competency, but some concepts with wider impact across IT security (e.g., privacy) were included in multiple competencies.

Step 4: Identify Generic IT Security Roles. After competencies were adequately populated with functions, and key terms and concepts were recognized, a set of generic roles performed by professionals in the IT security field were identified. Roles, rather than job titles, were chosen to eliminate IT sector-specific language and accurately capture the multitude of IT security positions in a way that would allow a practitioner to easily identify his or her role. For example, IT Security Compliance Officer is defined as a role—but its applicable job titles might include auditor, compliance officer, inspector general, or inspector. In some instances, a role may match an industry job title (i.e., Chief Information Officer [CIO]).

Step 5: Categorize Functions by Perspective (Manage, Design, Implement, or Evaluate). In this step, once roles had been identified competencies were revisited—specifically, the CWFs within each competency were categorized into one of the four functional perspectives of Manage, Design, Implement, or Evaluate. It is important to note that these perspectives do *not* convey a lifecycle concept of task or program execution as is typical of a traditional system development lifecycle (SDLC), but are used to sort functions of a similar nature. The functional perspectives are defined as follows:

- **Manage**: Functions that encompass overseeing a program or technical aspect of a security program at a high level, and ensuring currency with changing risk and threat environments.
- **Design**: Functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level.
- **Implement**: Functions that encompass putting programs, processes, or policies into action within an organization.
- **Evaluate**: Functions that encompass assessing the effectiveness of a program, policy, process, or security service in achieving its objectives.

Step 6: Map Roles to Competency to Functional Perspective. The final step in developing the complete EBK framework involved mapping the roles to appropriate sets of competencies and identifying the specific functional perspective that described work performed in that role. This activity created the IT Security Role, Competency, and Functional Matrix provided in Section 5. A conceptual, visual depiction of this 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 work within the Design functional perspective.

The premise behind this mapping and the competency/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. This work—from creating the strategy for a portion 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. Rather than all roles being responsible for knowing all areas of IT security and having the ability 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 by role through the four functional perspectives across a series of technical competency areas. It is on these functions that an individual should be evaluated if a role-based certification truly measures his or her ability to perform.

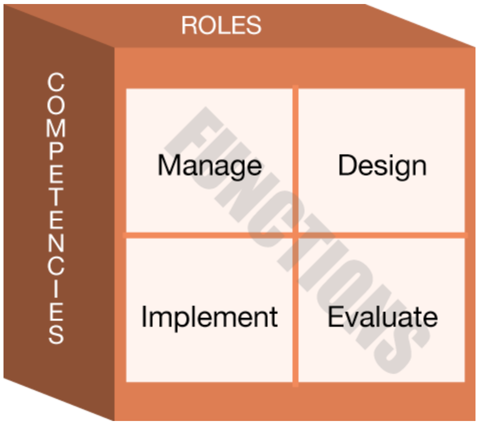


Figure 1-2: Roles to Competencies to Functions Mapping Diagram (Conceptual)

1.5 Review Cycle

The EBK conceptual framework (see page 44 for a full visual depiction) was shared with focus groups comprised of SMEs representing the private sector, government, and academia. These groups conducted analyses to ensure that the competencies, key terms and concepts, and roles were complete, and that they fully incorporated all aspects of the IT security discipline. Feedback was incorporated into a draft framework, which was presented to another, larger working group. This working group—which included both IT security generalists and SMEs who represented specific roles—reviewed the functional perspectives for each competency and role mapping. The resulting information was compiled to create the first draft of the EBK conceptual framework in December 2006.

DHS-NCSD introduced this first draft to a broader audience of SMEs in January 2007, which included 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 competencies and functional perspectives fully represented the specific role types. A broader review process continued through Fall 2007—this leveraged professional associations, industry conferences, sector-specific organizations, and culminated in the draft's submission to the Federal Register for public review and comment in October of that year. DHS-NCSD analyzed and aggregated the additional input into the *IT Security EBK*. It will be re-evaluated approximately every two years to ensure that content and overall structure remains relevant and useful.

1.6 Document Organization

The remaining sections of this document are organized as follows:

- ***Section 2: IT Security Competency Areas.*** This section contains the 14 competency areas, with their functional statements/definitions and work functions categorized according to the four functional perspectives—Manage, Design, Implement, and Evaluate.
- ***Section 3: IT Security Key Terms and Concepts.*** This section contains a list of the terms and concepts associated with each IT security competency area—please note that this is not meant to be an exhaustive list. Key terms and concepts identify the basic knowledge that professionals should have to be conversant in the field of IT security and 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 their related functional perspectives and competencies. Sample job titles are identified for each role to clarify those that align with each role—this allows individuals to identify where their particular role fits within the framework.
- ***Section 5: The IT Security Role, Competency, and Functional Matrix.*** This section contains a visual depiction of the relationship among roles, competencies, and functions.
- ***Appendix***. This section includes an acronym list and glossary pertaining to the *IT Security EBK*.

2 IT Security Competency Areas

This section describes the 14 competency areas with defining functional statements, and all work functions categorized as Manage, Design, Implement, or Evaluate.

2.1 Data Security

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

2.1.1 Manage

- Ensure that data classification and data management policies and guidance are issued and updated
- Specify policy and coordinate review and approval
- Ensure compliance with data security policies and relevant legal and regulatory requirements
- Ensure appropriate changes and improvement actions are implemented as required.

2.1.2 Design

- Develop data security policies using data security standards, guidelines, and requirements that include privacy, access, retention, disposal, incident management, disaster recovery, and configuration
- Identify and document the appropriate level of protection for data
- Specify data and information classification, sensitivity, and need-to-know requirements by information type
- Create authentication and authorization system for users to gain access to data by assigned privileges and permissions
- Develop acceptable use procedures in support of the data security policy
- Develop sensitive data collection and management procedures in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Identify an appropriate set of information security controls based on the perceived risk of compromise to the data
- Develop security testing procedures.

2.1.3 Implement

- Perform the data access management process according to established guidelines
- Apply and verify data security access controls, privileges, and associated profiles
- Implement media control procedures, and continuously monitor for compliance
- Implement and verify data security access controls, and assign privileges

- Address alleged violations of data security and privacy breaches
- Apply and maintain confidentiality controls and processes in accordance with standards, procedures, directives, policies, regulations, and laws (statutes).

2.1.4 Evaluate

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

2.2 Digital Forensics

Refers to the knowledge and understanding of digital investigation and analysis techniques used for acquiring, validating, 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 four phases: Prepare, 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 activities
- Provide adequate work spaces that at a minimum take into account the electrical, thermal, acoustic, and privacy concerns (i.e., intellectual properties, classification, contraband) and security requirements (including access control and accountability) of equipment and personnel, and provide adequate report writing/administrative areas
- Ensure appropriate changes and improvement actions are implemented as required
- Maintain current knowledge on forensic tools and processes.

2.2.2 Design

- Develop policies for the preservation of electronic evidence; data recovery and analysis; and the reporting and archival requirements of examined material in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Establish policies and procedures 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 and mobile toolkit
- Develop policies and procedures for preservation of electronic evidence; data recovery and analysis; and the reporting and archival requirements of examined material in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Establish 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 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, policies, regulations, and laws (statutes).

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 and maintain intrusion detection systems; intrusion prevention systems; network mapping software; and monitoring and logging systems; and analyze results to protect, detect, and correct information security-related vulnerabilities and events
- Follow proper chain-of-custody best practices in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- 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 relevant pieces of information from collected data
- Report complete and accurate findings, and result of the 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
- Advise on the suitability of Standard Operating Environment's (SOE) baseline standard for forensic analysis
- Coordinate applicable legal and regulatory compliance requirements
- Coordinate, interface, and work under the direction of appropriate corporate entities (e.g., corporate legal, corporate investigations) regarding 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 of forensic processes and accuracy of forensic tools used by digital forensic examiners, and implement changes as required
- Review all documentation associated with forensic processes or results for accuracy, applicability, and completeness
- Assess the effectiveness, accuracy, and appropriateness of testing processes and procedures followed by the forensic laboratories and teams, and suggest changes where appropriate
- Assess the digital forensic staff to ensure 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, peer review process, and audit 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 application of the principles, policies, and procedures used to ensure that an enterprise continues to perform essential business functions after the occurrence of a wide range of potential catastrophic events.

2.3.1 Manage

- Coordinate with corporate stakeholders to establish the enterprise continuity of operations program
- Acquire 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/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

- Ensure that appropriate changes and improvement actions are implemented as required
- Apply lessons learned from test, training and exercise, and crisis events.

2.3.2 Design

- Develop an enterprise continuity of operations plan and related 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 guidelines.

2.3.3 Implement

- Execute enterprise continuity of operations and related contingency plans and procedures
- Control access to information assets during an incident in accordance with organizational policy.

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 make recommendations for improvement
- Continuously validate the organization against additional mandates, as developed, to ensure full compliance
- Collect and report performance measures and identify improvement actions
- Execute crisis management tests, training, and exercises.

2.4 Incident Management

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

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 resources, including financial resources, for incident management functions

- Ensure 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
- Ensure that appropriate changes and improvement actions are implemented as required
- Establish an incident management measurement program.

2.4.2 Design

- Develop the incident management policy, based on standards and procedures for the organization
- Identify services that the incident response team should provide
- Create incident response plans in accordance with security policies and organizational goals
- Develop procedures for performing incident handling and reporting
- Create incident response exercises and penetration testing activities
- Develop specific processes for collecting and protecting forensic evidence during incident response
- Specify incident response staffing and training requirements
- Establish an incident management measurement program.

2.4.3 Implement

- Apply response actions in reaction to security incidents, in accordance with established policies, plans, and procedures
- Respond to and report incidents
- Assist in collecting, processing, and preserving evidence according to standards, procedures, directives, policies, regulations, and laws (statutes)
- Monitor network and information systems for intrusions
- Execute incident response plans
- Execute penetration testing 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
- Coordinate, integrate, and lead team responses with internal and external groups according to applicable policies and procedures.

2.4.4 Evaluate

- Assess the efficiency and effectiveness of incident response program activities, and make improvement recommendations

- Examine the effectiveness of penetration testing and incident response tests, training, and exercises
- Assess the effectiveness of communications between the incident response team and related internal and external organizations, and implement changes where appropriate
- Identify incident management improvement actions based on assessments of the effectiveness of incident management procedures.

2.5 IT Security Training and Awareness

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

2.5.1 Manage

- Identify business requirements and establish enterprise-wide policy for the IT security awareness and training program
- Acquire and manage 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 and requirements
- Ensure that appropriate changes and improvement actions are implemented as required.

2.5.2 Design

- Develop the security awareness and training policy for the IT security training and awareness program
- Define the goals and objectives of the IT security awareness and training program
- Work with appropriate security SMEs to ensure completeness and accuracy of the security training and awareness program
- Establish a tracking and reporting strategy for IT security training and awareness
- Establish a change management process to ensure currency and accuracy of training and awareness materials
- Develop a workforce development, training, and awareness program plan.

2.5.3 Implement

- Perform a needs assessment to determine skill gaps and identify critical needs based on mission requirements
- Develop new—or identify existing—awareness and training materials that are appropriate and timely for intended audiences
- Deliver awareness and training to intended audiences based on identified needs

- Update awareness and training materials when necessary
- Communicate management's commitment, and the importance of the IT security awareness and training program, to the workforce.

2.5.4 Evaluate

- Assess and evaluate the IT security awareness and training program for compliance with corporate policies, regulations, and laws (statutes), and measure program and employee performance against objectives
- Review IT security awareness and training program materials and recommend improvements
- Assess the awareness and training program to ensure that it meets not only the organization's stakeholder needs, but that it is effective and covers current IT security issues and legal requirements
- Ensure that information security personnel are receiving the appropriate level and type of training
- Collect, analyze, and report performance measures.

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. Individuals with this role perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are followed as intended.

2.6.1 Manage

- Establish security administration program goals and objectives
- Monitor the security administration program budget
- Direct 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 security administration team activities with other security-related team activities (e.g., technical support, incident management, security engineering)
- Acquire necessary resources, including financial resources, to execute the security administration program
- Ensure operational compliance with applicable standards, procedures, directives, policies, regulations, and laws (statutes)
- Ensure that IT systems operations and maintenance enables day-to-day business functions

- Ensure that appropriate changes and improvement actions are implemented as required.

2.6.2 Design

- Develop security administration processes and procedures in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Develop personnel, application, middleware, operating system, hardware, network, facility, and egress security controls
- Develop security monitoring, test scripts, test criteria, and testing procedures
- Develop security administration change management procedures to ensure that security policies and controls remain effective following a change
- Recommend appropriate forensics-sensitive policies for inclusion in the enterprise security plan
- Define IT security performance measures
- Develop a continuous monitoring process
- Develop role-based access, based on the concept of least privilege
- Maintain the daily/weekly/monthly process of backing up IT systems to be stored both on- and off-site in the event that a restoration should become necessary
- Develop a plan to measure the effectiveness of security controls, processes, policies and procedures.

2.6.3 Implement

- Perform security administration processes and procedures in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Establish a secure computing environment by applying, monitoring, controlling, and managing unauthorized changes in system configuration, software, and hardware
- Ensure that information systems are assessed regularly for vulnerabilities, and that appropriate solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented
- Perform security performance testing and reporting, and recommend security solutions in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Perform security administration changes and validation testing
- Identify, control, and track all IT configuration items through the continuous monitoring process
- Collaborate with technical support, incident management, and security engineering teams to develop, implement, control, and manage new security administration technologies
- Monitor vendor agreements and Service Level Agreements (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 (statutes) and regulations

- Perform proactive security testing.

2.6.4 Evaluate

- Review strategic security technologies
- Review performance and correctness of applied security controls in accordance with standards, procedures, directives, policies, regulations, and laws (statutes), and apply corrections as required
- Assess the performance of security administration measurement technologies
- Assess system and network vulnerabilities
- Assess compliance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Identify improvement actions based on reviews, assessments, and other data sources
- Collect IT security performance measures to ensure optimal system performance.

2.7 Network and Telecommunications Security

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

2.7.1 Manage

- Establish a network and telecommunications security program in line with enterprise goals and policies
- Manage the necessary resources, including financial resources, to establish and maintain an effective network and telecommunications security program
- Direct network and telecommunications security personnel
- Define the scope of the network and telecommunications security program
- Establish communications between the network and telecommunications security team and related security teams (e.g., technical support, security administration, incident response)
- Establish a network and telecommunications performance measurement and monitoring program
- Ensure enterprise compliance with applicable network-based standards, procedures, directives, policies, regulations, and laws (statutes)
- Ensure that network-based audits and management reviews are conducted to implement process improvement
- Ensure that appropriate changes and improvement actions are implemented as required.

2.7.2 Design

- Develop network and host-based security policies in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Specify strategic security plans for network telecommunications in accordance with established policy, to meet organizational security goals
- Develop network and telecommunications security operations and maintenance standard operating procedures
- Develop effective network domain security controls in accordance with enterprise, network and host-based policies
- Develop network security performance reports
- Develop network security and telecommunication audit processes, guidelines, and procedures.

2.7.3 Implement

- Prevent and detect intrusions, and protect against malware
- Perform audit tracking and reporting
- Apply and manage effective network domain security controls in accordance with enterprise, network, and host-based policies
- Test strategic network security technologies for effectiveness
- Monitor and assess network security vulnerabilities and threats using various technical and non-technical data
- Mitigate network security vulnerabilities in response to problems identified in vulnerability reports
- Provide real-time network intrusion response
- Ensure that messages are confidential and free from tampering and repudiation
- Defend network communications from tampering and/or eavesdropping
- Compile data into measures for analysis and reporting.

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
- Assess fulfillment of functional requirements by arranging independent verification and validation of the network
- Analyze data and report results
- Ensure that anti-malware systems are operating correctly
- 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. These controls include organization/functional design elements such as separation of duties, job rotation, and classification.

2.8.1 Manage

- Coordinate with IT security, physical security, operations security, and other organizational managers to ensure a coherent, coordinated, and holistic approach to security across the organization
- Ensure personnel security compliance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Acquire and manage the necessary resources, including financial resources, to maintain effective personnel security
- Establish objectives for personnel security to ensure alignment with 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 ongoing operations of the personnel security program
- Ensure that appropriate changes and improvement actions are implemented as required
- Ensure personnel security compliance with standards, procedures, directives, policies, regulations, and laws (statutes).

2.8.2 Design

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

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 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 organizational requirements, 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/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.

2.8.4 Evaluate

- Review effectiveness of the personnel security program, and recommend changes that will improve internal practices and/or security organization-wide
- Assess the relationships between personnel security procedures and organization-wide security needs, and make recommendations for improvement
- Periodically review the personnel security program for compliance with standards, procedures, directives, policies, regulations, and laws (statutes)

2.9 Physical and Environmental Security

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

2.9.1 Manage

- Coordinate with personnel managing IT security, personnel security, operations security, and other security functional areas to provide an integrated, holistic, and coherent security effort
- Acquire 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 the impact if unavailable
- Ensure that appropriate changes and improvement actions are implemented as required.

2.9.2 Design

- Identify the physical security program requirements and specifications in relationship to enterprise security goals
- Develop policies and procedures for identifying and mitigating physical and environmental threats to information assets, personnel, facilities, and equipment
- Develop a physical security and environmental security plan, including security test plans and contingency plans, in coordination with other security planning functions
- Develop countermeasures against identified risks and vulnerabilities

- Develop criteria for inclusion in the acquisition of facilities, equipment, and services that impact physical security.

2.9.3 Implement

- Apply physical and environmental controls in support of physical and environmental security plans
- Control access to information assets in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Integrate physical security concepts into test plans, procedures, and exercises
- Conduct threat and vulnerability assessments to identify physical and environmental risks and vulnerabilities, and update applicable controls as necessary
- Review construction projects to ensure that appropriate physical security and protective design features are incorporated into their design
- Compile, analyze, and report performance measures.

2.9.4 Evaluate

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

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 (SLA), justifications required by policies or procedures, and contract administration plans.

2.10.1 Manage

- Collaborate with various stakeholders (which may include internal client, lawyers, CIOs, Chief Information Security Officers, IT security professionals, privacy professionals, security engineers, suppliers, and 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
- Ensure that investments are aligned with enterprise architecture and security requirements
- Conduct detailed IT investment reviews and security analyses, and review IT investment business cases for security requirements
- Ensure that the organization's IT contracts do not violate laws and regulations, and require compliance with standards when applicable
- Specify policies for use of third party information by vendors/partners, and connection requirements/acceptable use policies for vendors that connect to networks
- Ensure that appropriate changes and improvement actions are implemented as required
- Whenever applicable, calculate return on investment (ROI) of key purchases related to IT infrastructure and security.

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 requirements, 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 and evaluate 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) to include IT security requirements that minimize risk to the organization
- Ensure that physical security concerns are integrated into acquisition strategies
- Maintain ongoing and effective communications with suppliers and providers
- Perform compliance reviews of delivered products and services to assess the delivery of IA 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-applicable IT security trends, including practices for mitigating security risks associated with supply chain management
- Review Memoranda of Agreement, Memoranda of Understanding, and/or SLA for agreed levels 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 internal policy with regard to use of third party information and connection requirements
- Conduct due diligence activities to ensure that vendors are operationally and technically competent to receive third party information, connect and communicate with networks, and deliver and support secure applications
- Evaluate the effectiveness of procurement function in 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 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 (statutes)
- Define the enterprise information security compliance program
- Coordinate and provide liaison with staffs that are responsible for information security compliance, licensing and registration, and data security surveillance
- Identify and stay current on all external laws, regulations, standards, and best practices applicable to the organization
- Identify major enterprise risk factors (product, compliance, and operational) 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, and stakeholders
- Keep informed on pending information security changes, trends, and best practices by participating in collaborative settings

- Acquire the necessary resources to support an effective information security compliance program
- Establish an enterprise information security compliance performance measures program
- Ensure that appropriate changes and improvement actions are implemented 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 (statutes)
- Specify enterprise information security compliance program control requirements
- Author information security compliance performance reports
- Develop a plan of action and associated mitigation strategies to address program deficiencies
- Develop a compliance reporting process in a manner that produces evidence that a process exists.

2.11.3 Implement

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

2.11.4 Evaluate

- Assess the effectiveness of enterprise compliance program controls against applicable standards, policies, procedures, guidelines, directives, regulations, and laws (statutes)
- Assess 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 Security Risk Management

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

2.12.1 Manage

- Establish a IT security risk management program based on enterprise business goals and objectives
- Establish the risk assessment process
- Advise senior management on the impact 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
- Make determination on acceptance of residual risk
- Ensure that appropriate changes and improvement actions are implemented as required.

2.12.2 Design

- Specify risk-based information security requirements and a security concept of operations
- Develop policies, processes, and procedures for identifying, assessing, and mitigating risks to information assets, personnel, facilities, and equipment
- Develop processes and procedures for determining the costs and benefits of risk mitigation strategies
- Develop procedures for documenting the decision to apply mitigation strategies or acceptance of risk
- Develop and maintain risk-based security policies, plans, and procedures based on security requirements and in accordance with standards, procedures, directives, policies, regulations, and laws (statutes).

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

2.12.4 Evaluate

- Assess effectiveness of the risk management program, and implement changes where required
- Review the performance of, and provide recommendations for, risk management (e.g., security controls, policies/procedures that make up risk management program) tools and techniques
- Assess residual risk in the information infrastructure used by the organization

- Assess the results of threat and vulnerability assessments to identify security risks, and regularly update applicable security controls
- Identify changes to risk management policies and processes that will enable them to remain current with the emerging risk and threat environment.

2.13 Strategic Security 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 security management requires the practice of external business analyses such as customer analyses, competitor analyses, market analyses, and industry environmental analyses. It also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities/constraints. The goal of these analyses is to ensure that an organization’s IT security principles, practices, and system design are in line with its 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 that 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 and manage the necessary resources, including financial resources, to support IT security goals and objectives and reduce overall organizational risk
- Establish overall enterprise information security architecture (EISA) 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 security policy elements in the operational environment
- Establish organizational goals that are in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Balance the IT security investment portfolio based on EISA considerations and enterprise security priorities
- Ensure appropriate changes and improvement actions are implemented as required.

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 organization’s business/mission needs
- 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 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 the IT portfolio to determine if funding accurately aligns with security goals and objectives, and make funding recommendations accordingly
- Assess the integration of security with business/mission, and recommend improvements
- Review cost goals of each major investment
- Assess performance and overall effectiveness of the security program with respect to security goals and objectives
- Assess and refresh the 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 SDLC prior to the Operations and Maintenance phase. This approach ensures that the operation of IT systems and software does not present undue risk to the enterprise and its information assets. Supporting activities include 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 integration of security in the SDLC
- Guide IT security personnel through the SDLC phases
- Provide feedback to developers on security issues through the SDLC

- Define the scope of the IT security program as it applies to application of the SDLC
- Plan the IT security program components into the SDLC
- Collaborate with IT project management to integrate security functions into the project management process
- Ensure that appropriate changes and improvement actions are implemented as required.

2.14.2 Design

- Specify the enterprise and IT system or application security policies, standards, and best practices
- Specify 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 standards against which to engineer 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, procedures, guidelines, directives, regulations, and laws (statutes).

2.14.3 Implement

- Execute the enterprise and IT system or application security policies
- Apply and verify compliance with identified standards against which to engineer the IT system or application
- Perform processes and procedures to mitigate the introduction of vulnerabilities during the engineering process
- Perform configuration management practices
- Validate that 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
- Implement and test backup-and-restore procedures for critical systems.

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 SDLC phases
- Continually assess 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 IT Security Key Terms and Concepts

The purpose of this listing is to provide a basic understanding of key terms and concepts rather than offer an exhaustive list. Knowledge of these terms and concepts is the foundation for effective performance of functions associated with each of the technical competency areas.

The *IT Security EBK* lists all the key terms and concepts that have been identified for each competency area. At minimum, individuals should know, understand, and be able to apply those that relate to the competencies to which their role is linked. Full knowledge of all of the 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 and their affiliated key terms and concepts.

3.1 Data Security

Refers to the application of 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.

- Access Control
- Aggregation
- Antivirus Software
- Authentication
- Authorization
- Data Classification
- Decryption
- Digital Signatures
- Discretionary Access Control
- Electronic Commerce
- Encryption
- Firewall Configuration
- Identity Data and Access Management
- Identity Management
- Information Classification Scheme
- Least Privilege
- 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 Record
- User Privileges
- User Provisioning

3.2 Digital Forensics

Refers to the knowledge and understanding of digital investigation and analysis techniques used for acquiring, validating, 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 four phases: Prepare, Acquire, Analyze, and Report.

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

3.3 Enterprise Continuity

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

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

3.4 Incident Management

Refers to knowledge and understanding of the process to prepare and prevent, detect, contain, eradicate, 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 Stakeholder
- Information System
- Intrusion
- Measures
- Personally Identifiable Information (PII)
- Reconstitution of System
- Risk
- Risk Assessment
- Risk Management
- Security Alerts
- Security Incident
- System Compromise
- Threat Motivation
- Unauthorized Access
- Vulnerability

3.5 IT Security Training and Awareness

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

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

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. Individuals with this role perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are followed as intended.

- Access Control
- Antivirus Software
- Backup
- Baseline
- Configuration Management
- Insider Threat
- Intrusion Detection System
- Intrusion Prevention System
- Patch Management
- Penetration Testing
- Security Data Analysis
- Security Measures
- Security Reporting
- System Hardening
- System Logs
- System Monitoring
- Threat Analysis
- Threat Monitoring
- Vulnerability Analysis

3.7 Network and Telecommunications Security

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

- Access Control
- Authentication
- Communications Security (COMSEC)
- Configuration
- Cryptosecurity
- Defense-in-Depth
- Emission Security
- Encryption Technologies (e.g., Secure Sockets Layer [SSL], Transport Layer Security [TLS])
- Firewall
- Hub
- Intrusion Detection System
- Intrusion Prevention Systems
- Load Balancers
- Network Architecture
- Networking Models and Protocols (i.e.: Open Systems Interconnection (OSI) or TCP/IP)
- Network Segmentation (e.g., Virtual Local Area Network [V-LAN], Demilitarized Zone [DMZ])
- Penetration Testing
- Port
- Router
- Security Trust
- Switch
- Telecommunications Technology (e.g., Private Branch Exchange [PBX] and Voice Over Internet Protocol [VOIP])
- Transmission Security
- Virtual Private Network (VPN)
- Vulnerability
- Web Services Security
- Wired and Wireless Networks

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. Controls include organization/functional design elements such as separation of duties, job rotation, and classification.

- Background Checks/Background Investigation
- Confidentiality
- Digital Identity
- Human Resources
- Insider Threat
- Job Rotation
- Nondisclosure Agreement
- Position Sensitivity
- Security Breach
- Security Clearance
- Separation of Duties
- Social Engineering
- Special Background Investigation (SBI)
- Suitability Determination

3.9 Physical and Environmental Security

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

- Access Cards
- Access Control
- Alarm
- Asset Disposal
- Biometrics
- Defense-in-Depth
- Environmental Threat
- Identification and Authentication
- Inventory
- Manmade Threat
- Natural Threat
- Perimeter Defense
- Risk Management
- Threat and Vulnerability Assessment
- Video Surveillance

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, 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, SLAs, justifications required by policies or procedures, and contract administration plans.

- Acceptable Risk
- Acquisition
- Acquisition Life Cycle
- Business Impact Analysis
- Contract
- Cost-Benefit Analysis
- Disposal
- Prequalification
- Regulatory Compliance
- Request for Information
- Request for Proposal (RFP)
- Risk Analysis
- Risk-Based Decision
- Risk Mitigation
- Security Requirements
- Service Level Agreement (SLA)
- Solicitation
- Statement of Objectives (SOO)
- Statement of Work (SOW)
- Total Cost of Ownership (TCO)

3.11 Regulatory and Standards Compliance

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

- Accountability
- Assessment
- Auditing
- Certification
- Compliance
- Ethics
- Evaluation
- Governance
- Laws (including but not limited to the Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, 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 Information Practices
- Procedure
- Regulations
- Security Program
- Standards (e.g., ISO 27000 series, Federal Information Processing Standards [FIPS])
- Validation
- Verification

3.12 Security Risk Management

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

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

3.13 Strategic Security 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 security management requires the practice of external business analyses such as customer analyses, competitor analyses, market analyses, and industry environmental analyses. It also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities/constraints. The goal of these analyses is to ensure that an organization’s IT security principles, practices, and system design are in line with its 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

3.14 System and Application Security

Refers to 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.

- Accreditation
- Application Controls
- Baseline Security
- Certification
- Configuration Management
- Patch Management
- Process Maturity
- Risk Assessment
- Risk Mitigation
- Secure Coding
- Secure Coding Principles
- Secure Coding Tools
- Secure System Design
- Security Change Management
- Security Requirements Analysis
- Security Specifications
- Security Testing and Evaluation
- Security Vulnerability Analysis
- Software Assurance
- System Development Life Cycle (SDLC)
- System Engineering
- Technical Security Controls

4 IT Security Roles, Competencies, and Functional Perspectives

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

4.1 Chief Information Officer

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

Competencies:

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

Example Job Titles:

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

4.2 Digital Forensics Professional

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

Competencies:

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

- Security Risk Management: *Implement*

Example Job Titles:

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

4.3 Information Security Officer

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

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*
- Personnel Security: *Manage*
- Physical and Environmental Security: *Manage, Evaluate*
- Procurement: *Manage, Design, Evaluate*
- Regulatory and Standards Compliance: *Manage, Design, Evaluate*
- Security Risk Management: *Manage, Design, Evaluate*
- Strategic Security Management: Manage, Design, *Implement*, *Evaluate*
- System and Application Security: *Manage, Evaluate*

Example Job Titles:

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

4.4 IT Security Compliance Officer

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

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 and Telecommunications Security: *Evaluate*
- Personnel Security: *Evaluate*
- Physical and Environmental Security: *Evaluate*
- Procurement: *Evaluate*
- Regulatory and Standards Compliance: *Design, Implement, Evaluate*
- Security Risk Management: *Implement, Evaluate*
- Strategic Security 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 and Telecommunications Security: *Design, Implement*
- Security 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 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*
- Security Risk Management: *Design*, *Implement*, *Evaluate*

Example Job Titles:

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

4.7 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 and Telecommunications Security: *Manage, Design, Implement, Evaluate*

- Procurement: *Evaluate*
- Security 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

4.8 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: *Evaluate*
- Security Risk Management: *Implement*

Example Job Titles:

- Facility Security Officer
- 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. He or she establishe**s** a risk management framework and governance model to assure the appropriate handling of Personally Identifiable Information (PII**)**, and ensures that 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*
- Security 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 (e.g., software, hardware) and services (e.g., contractor support) in support of an organization's IT strategy. In the IT security context, they must ensure that security requirements are specified within solicitation and contract documents (Sarbanes-Oxley, FISMA) and that only products and services meeting requirements are procured. Procurement Professionals must be knowledgeable about their industry and own organization, and must be able to effectively communicate with suppliers and negotiate terms of service.

Competencies:

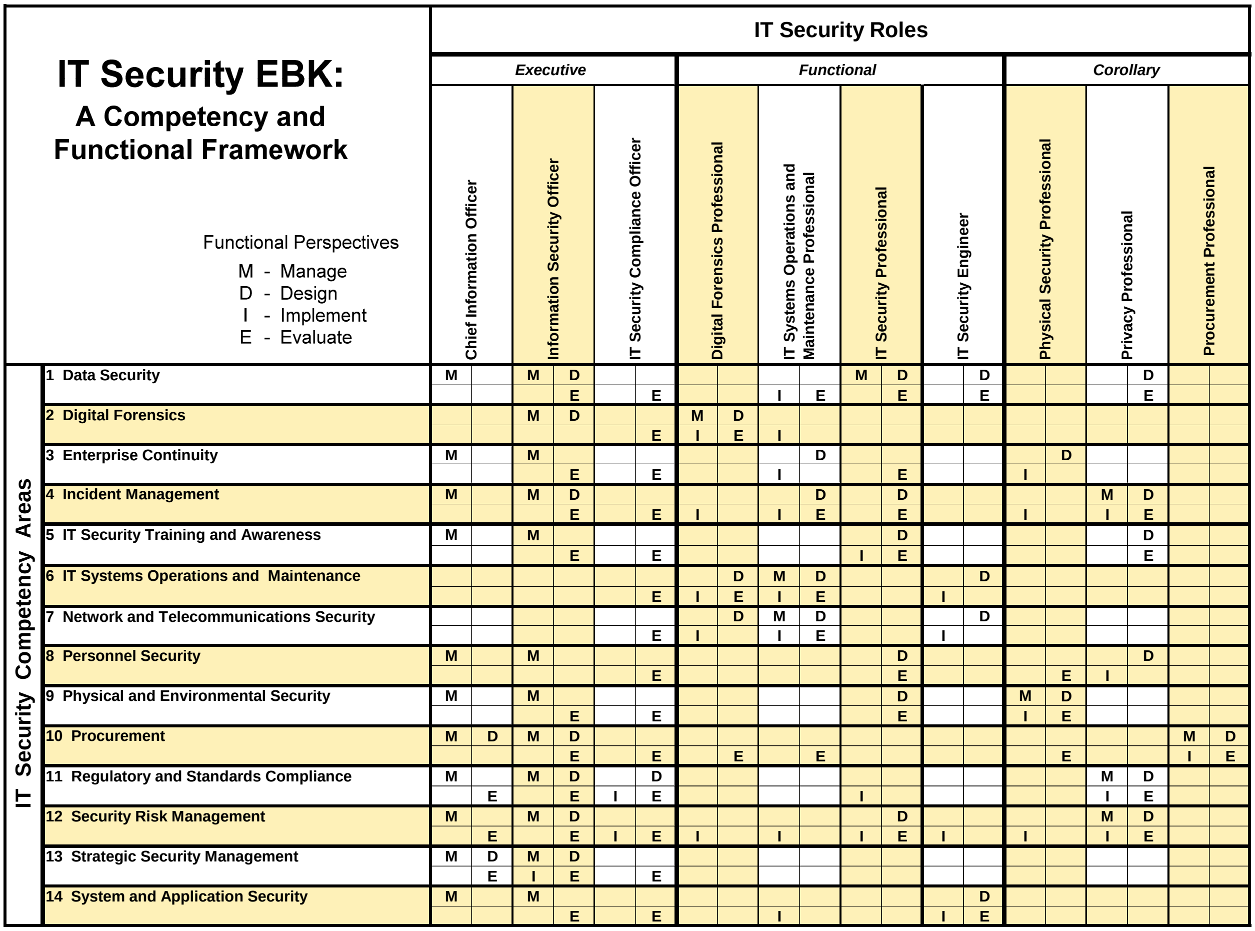
- Procurement: *Manage, Design, Implement, Evaluate*

Example Job Titles:

- Acquisition Manager
- Buyer
- Contracting Officer
- Contracting Officer's Technical Representative (COTR)
- Contract Specialist
- Purchasing Manager

5 The 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, IT security roles are broadly grouped into Executive, Functional, and Corollary categories.



IT Security EBK:
A Competency and Functional Framework

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

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

Figure 1-3: The IT Security Role, Competency, and Functional Matrix

6 Appendix: List of Acronyms

Acronym	Definition
A	
A/R	Actions/Recommendations
C	
C&A	Certification and Accreditation
CBT	Computer Based Training
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
COBIT	Control Objectives for Information and related Technology
COMSEC	Communications Security
COTR	Contracting Officer's Technical Representative
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	
EISA	Enterprise Information Security Architecture
EBK	Essential Body of Knowledge
F	
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
H	
HIPAA	Health Insurance Portability and Accountability Act
I	
IA	Information Assurance

Acronym	Definition
IAM	Information Assurance Manager
IASO	Information Assurance Security Officer
IASS	Information Assurance Skill Standard
ILT	Instructor Led Training
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
O	
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
P	
PBX	Private Branch Exchange
PCIPB	President’s Critical Infrastructure Protection Board
PII	Personally Identifiable Information
R	
RFP	Request for Proposal
ROI	Return on Investment
S	
SBI	Special Background Investigation
SDLC	System Development Life Cycle

Acronym	Definition
SLA	Service Level Agreement
SME	Subject Matter Expert
SOE	Standard Operating Environment
SOO	Statement of Objectives
SOW	Statement of Work
SSE CMM	Systems Security Engineering Capability Maturity Model
SSL	Secure Sockets Layer
T	
T/E	Training and Education (Program)
TCO	Total Cost of Ownership
TLS	Transport Layer Security
V	
V-LAN	Virtual Local Area Network
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
W	
WBT	Web Based Training