# NIST Special Publication 800-16

**Revision 1 (3rd Draft)**

A Role-Based Model for Federal Information Technology/ Cybersecurity Training

Patricia Toth Penny Klein

**I N F O R M A T I O N S E C U R I T Y**



# NIST Special Publication 800-16

**Revision 1 (3rd Draft)**

A Role-Based Model for



**Federal Information Technology/**

**Cybersecurity Training**

Patricia Toth *Computer Security Division Information Technology Laboratory*

Penny Klein *Systegra, Inc. Leesburg, Virginia*

March 2014

U.S. Department of Commerce

*Penny Pritzker, Secretary*

National Institute of Standards and Technology

*Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director*

**Authority**

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information technology/cybersecurity standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to National Security Systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-16 Natl. Inst. Stand. Technol. Spec. Publ. 800-16, 144 pages (March 2014) <http://dx.doi.org/10.6028/NIST.SP.XXX>

CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at [http://csrc.nist.gov/publications.](http://csrc.nist.gov/publications)

###### Public comment period: March 14, 2014 through April 30, 2014

National Institute of Standards and Technology

Attn: Computer Security Division, Information Technology Laboratory 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930 Email: [ptoth@nist.gov](mailto:ptoth@nist.gov)

**Reports on Computer Systems Technology**

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

**Abstract**

Meeting security responsibilities and providing for the confidentiality, integrity, and availability of information in today's highly networked environment can be a difficult task. Each individual that owns, uses, relies on, or manages information and information technology (IT) systems must fully understand their specific security responsibilities. This includes ownership of the information and the role individuals have in protecting information. Information that requires protection includes information they own, information provided to them as part of their work and information they may come into contact with.

This document describes information technology/cybersecurity role-based training for the Federal Departments and Agencies and Organizations (Federal Organizations) and contractor support in these roles. Its primary focus is to provide a comprehensive, yet flexible, training methodology for the development of training courses or modules for personnel who have been identified as having significant information technology/cybersecurity responsibilities. This document is intended to be used by Federal information technology/cybersecurity training personnel and their contractors to assist in designing role-based training courses or modules for Federal Organizations personnel and contractors who have been identified as having significant responsibilities for information technology/cybersecurity. This publication should also be read, reviewed, or understood at a fairly high level by several audiences including the Organizational Heads through the leadership chain to the individual. Some of the titles include, but not limited to, the IT Managers, Senior Agency Information Security Officer (SAISO), Certified Information Systems Security Officer (CISSO), Information Systems Security Officer (ISSO), Information Assurance Manager (IAM), and Program Manager (PM).

**Keywords**

Cybersecurity; information assurance; learning continuum; role-based training; security; security awareness; security controls; security literacy

**Acknowledgements**

NIST wishes to thank the members of the Federal Information Systems Security Educators’ Association (FISSEA) Technical Working Group (TWG) who provided input and confirmation of various concepts that led to this version of the document.

NIST also wishes to thank all individuals, Federal Organizations and Companies that contributed to the first round of review and provided input to this version of the document.

**Notes to Reviewers**

NIST SP 800-16, *A Role-Based Model for Federal Information Technology/Cybersecurity Training* is intended to be used by Federal information technology/cybersecurity training personnel and their contractors to assist in designing role-based training courses or modules for Federal Organization personnel who have been identified as having significant responsibilities for information technology/cybersecurity.

**Table of Contents**

[Executive Summary 7](#_bookmark0)

[Chapter 1 - Introduction 8](#_bookmark1)

* 1. [Who should understand NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training”*? . 10](#_bookmark2)
  2. [Legislative and Policy Drivers 11](#_bookmark3)
  3. [Relationships with Other NIST Documents 12](#_bookmark4)
  4. [Scope 13](#_bookmark5)
  5. [Audience 13](#_bookmark6)
  6. [Assumptions 14](#_bookmark7)
  7. [DocumentOrganization 16](#_bookmark8)

[Chapter 2 – Perspectives 18](#_bookmark9)

[Chapter 3 Organizational Responsibilities 21](#_bookmark10)

* 1. [Organizational Responsibilities 21](#_bookmark11)
  2. [Organization Head 21](#_bookmark12)
  3. [Chief Information Officer (CIO) 21](#_bookmark13)
  4. [Senior Agency Information Security Officer (SAISO) 22](#_bookmark14)
  5. [Cybersecurity Training Manager/Chief Learning Officer (CLO) 22](#_bookmark15)
  6. [Managers 22](#_bookmark16)
  7. [Training Developer/Instructional Design Specialists 23](#_bookmark17)
  8. [Personnel with Significant IT/ Cybersecurity Responsibilities 23](#_bookmark18)
  9. [Users 23](#_bookmark19)

[Chapter 4 – Cybersecurity Learning Continuum 25](#_bookmark20)

* 1. [Security Awareness 28](#_bookmark21)
  2. [Role-Based Training 31](#_bookmark22)
  3. [Education and Experience 34](#_bookmark23)
  4. [Role-Based Training Differs From Other Types of Training 35](#_bookmark24)

[Chapter 5 – Role-Based Training Methodology 38](#_bookmark25)

* 1. [Role-Based Training 38](#_bookmark26)
  2. [Developing and Implementing Role-Based Training 39](#_bookmark27)
  3. [Understanding the Role-Based Training Methodology 43](#_bookmark28)

[Chapter 6 – Worked Example 46](#_bookmark29)

[Chapter 7 – Training Evaluation 49](#_bookmark30)

* 1. [Value of Evaluation in a Training Program 49](#_bookmark31)
  2. [Purpose of Training Evaluation 49](#_bookmark32)
  3. [Development of an Evaluation Plan 50](#_bookmark33)

[Appendix A: Functions 56](#_bookmark34)

[Appendix B: Knowledge and Skills Catalog 65](#_bookmark35)

[Appendix C: Roles 82](#_bookmark36)

[Appendix D: Sample Evaluation Forms 147](#_bookmark37)

[Appendix E: Glossary 158](#_bookmark38)

[Appendix F: Acronyms 160](#_bookmark39)

[Appendix G: References 161](#_bookmark40)

# Executive Summary

Some of the most effective current attacks on cyber networks world-wide exploit user behavior. These include phishing attacks, social engineering to obtain passwords, and introduction of malware via removable media. These attacks and increased complexities demand greater focus on training to the IT staff to avoid misconfigurations, bolster hardening and increase response. Training users (privileged and unprivileged) and those with access to other pertinent information and media is a necessary deterrent to these methods. Therefore, in conjunction with Federal Information Security Management Act (FISMA) requirements, role-based training of those individuals with significant responsibility is required.

All Federal Organizations are required to have a security program implemented. There are many aspects included in the overall program. NIST guidance, NIST 800-50, “*Building an Information Technology Security Awareness and Training Program*” identifies aspects of an effective training program. There are multiple initiatives and guidance to assist with building an information technology/cybersecurity program, such as the National Initiative for Cybersecurity Education (NICE). The role-based training requirement is a piece of this higher level program. Chapter 2 of this document provides more detail on the difference between education and role-based training, and why role-based training is critical to a successful security training program.

Meeting security responsibilities and providing for the confidentiality, integrity, and availability of information in today's highly networked environment can be a difficult task. Each individual that owns, uses, relies on, or manages information and information systems must fully understand their specific security responsibilities. This includes ownership of the information and the role individuals have in protecting information. Information that requires protection includes:

* Information they own;
* Information provided to them as part of their work; and
* Information they may come into contact with.

This document, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training”* describes a process to develop information technology/cybersecurity role-based training. Its primary focus is to provide a comprehensive, yet flexible, training methodology for the development of training courses or modules for personnel who have been identified as having significant information technology/cybersecurity responsibilities within Federal Organizations. It should be stressed that this is guidance and the Federal Organizations are expected to tailor the role-based training to meet the needs of their own organization.

This document is intended to be used by Federal information technology/cybersecurity training personnel and their contractors to assist in designing role-based training courses or modules for Federal personnel who have been identified as having significant responsibilities for information technology/cybersecurity. This publication should also be read, reviewed, or understood at a fairly high level by Heads of Federal Organizations down through the leadership chain to the Information Technology (IT) individual. This includes several audiences including IT Managers, Senior Agency Information Security Officer (SAISO), Certified Information Systems Security Officer (CISSO), Information Systems Security Officer (ISSO), Information Assurance Manager (IAM), and Program Manager (PM).

# Chapter 1 - Introduction

The Federal government must protect its information and assets. Federal laws, policies, standards, directives, regulations and guidance task individuals within Federal departments and agencies – from heads of Federal Organizations to end users, and every level in between – with a variety of security responsibilities. These responsibilities include:

* Protecting and safeguarding information;
* Identifying and categorization of systems;
* Assigning impact levels to the systems and to the information stored in and processed by those systems;
* Selecting and implementing appropriate security controls;
* Testing the effectiveness of the security controls;
* Authorizing the use of the systems;
* Authorizing access to systems;
* Maintaining an effective information technology/cybersecurity posture by continuous monitoring; and
* Carrying out their specific role based security-related responsibilities.

Meeting these security responsibilities and providing for the confidentiality, integrity, and availability of information in today's highly networked environment can be a challenging task. Each individual that owns, uses, relies on, or manages information and information systems must fully understand their specific security responsibilities. All managers must ensure that all users are provided awareness training, and that those identified as having significant responsibilities for information technology/cybersecurity are appropriately trained based on the requirements of the Federal Organization. Senior Management/Leadership needs to support the role-based training. Chapter 2 provides more clarification on how the role-based training plays a critical role in the overall security training program.

Before proceeding further it is important to define key terms that will be used and discussed. These definitions are for use in this document and have been developed to provide clarity to the reader.

Additional definitions can be found in Appendix E, Glossary.

*Awareness* - the ability of the user to recognize or avoid behaviors that would compromise cybersecurity; practice of good behaviors that will increase cybersecurity; and act wisely and cautiously, where judgment is needed, to increase cybersecurity.

*Awareness Training* – consists of instructor led, on-line courses, exercises or other methods that inform users of acceptable use of and risk to the organization’s organizations systems.

*Base knowledge* - the familiarity, awareness, or understanding of security gained through experience or study

*Competency* – being qualified based on demonstration of an acceptable level of skills

*Cybersecurity Essentials -* the transitional stage between “Basic Awareness” and “Role-based Training.” It provides the foundation for subsequent specialized or role-based training by providing a universal

baseline of key security terms and concepts

*Education* - knowledge or skill obtained or developed by a learning process

*Job Function* - action for which a person or thing is particularly fitted or employed

*Knowledge Unit* – the combination of information needed to perform a function or activity effectively and efficiently

*Proficiency -* the state or quality of being competent

*Role* - the responsibility and functions that a person is currently performing within their organization

*Skills –* combination of ability, knowledge, and experience that enables a person to do something well

*Training* - the action provided to a user in the acquisition of knowledge, skills, and competencies in the security arena

Roles are established by the individual Federal Organization and Agencies through position descriptions, hierarchy charts, responsibilities, etc. These Federal Organization defined roles can be matched to the generic roles used in the role-based training methodology. Roles with security related responsibilities may not be clearly stated within organizations. Everyone has a responsibility in security even if their role does not specifically state security responsibilities. For example, managers who serve as owners of systems and applications have responsibility for the overall information technology/cybersecurity of those systems (i.e., security of general support systems, applications, networks).

All employees must be exposed to information technology/cybersecurity awareness material. All users of information systems must receive awareness training, as required by FISMA. This awareness training helps to shape user behavior to be more secure. In today’s environment, the most effective attacks on systems and networks are often via the exploitation of user behavior.

This document and NIST SP 800-50, “*Building an Information Technology Security Awareness and Training Program,”* describe the following key approaches of an information technology/cybersecurity awareness and training program that “Federal Organizations” (e.g., Federal agency/departments, Agencies or organizations) should follow to help ensure that individuals learn the appropriate information technology/cybersecurity-related material:

* All employees of an organization must be regularly or continually exposed to information technology/cybersecurity awareness. Security awareness techniques may include posters, awareness tools/trinkets, periodic e-mails, warning messages, “tips of the day” upon accessing an information system, or information technology/cybersecurity events;
* All users of information and information systems must attend information technology/cybersecurity awareness training (on-line or in-person) each year. This material should provide cybersecurity Essentials; and
* Individuals identified by their organization as having significant responsibility for information technology/cybersecurity must receive formal role-based information technology/cybersecurity training.

NIST SP 800-50, “*Building an Information Technology Security Awareness and Training Program*” provides guidance for building an effective IT security program and supports requirements specified

in FISMA and the Office of Management and Budget (OMB) *Circular A-130, Appendix III*. A strong IT security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources. In addition, those in the agency who manage the IT infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to security training puts an enterprise at great risk because security of agency resources is as much a human issue as it is a technology issue. An IT/cybersecurity training program should also strive to cultivate an IT/cybersecurity environment where behaviors and responses evolve to the point where they become automatic and consistent across the environment.

* 1. **Who should understand NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training”*?**

Chief Information Officers (CIO) and other executives should refer to this document to gain a basic understanding, beyond what is mentioned in NIST SP 800-50*, “Building an Information Technology Security Awareness and Training Program*” of their organization’s responsibilities regarding IT/cybersecurity role-based training. An organization’s CIO should understand that NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training,”* can be used to develop information systems/cybersecurity courses or modules to meet FISMA awareness role-based training requirement

The SAISO, IT/cybersecurity program managers and staff, senior managers and auditors should also be familiar with the scope of this document and understand the applicability of Cybersecurity Essentials and the role-based courses or modules for those who have been identified as having significant responsibilities for IT/cybersecurity. The SAISOs and other IT/cybersecurity practitioners should use this document to determine when they give responsibility for material development to training developers/Instructional Design Specialists (IDS).

Other personnel will need to work together to meet their responsibilities which include, but not limited to:

* + - Management: All levels of management will be responsible for their staff training needs; prioritize the use of training resources, identify training gaps and evaluate the training effectiveness within the work space;
    - IT/Cybersecurity Specialist: The IT/Cybersecurity specialist will be responsible for assisting, as a Subject Matter Expert (SME), in identifying training courses and training aids to meet the requirements of the roles or job functions; identify training gaps and needs within the organization’s IT/Cybersecurity program; contributes to determining any customization that is needed and developing a compliance baseline for the organization; and
    - Training Professionals: This group includes human resource planners, training coordinators/curriculum developers, course developers/IDS, and, of course the trainers responsible for developing, presenting and evaluating the training. This document will assist the training profession in understanding the IT security requirements and knowledge/skills required; evaluate the course quality; obtain the appropriate courses and materials; develop or customize courses/materials; and tailor their teaching approach to achieve the desired Learning Objectives.

## Legislative and Policy Drivers

FISMA was signed into law in 2002, fine-tuned long-standing information technology awareness and training requirements. FISMA clearly distinguishes between awareness efforts and training. Regarding awareness, FISMA states that an agency wide information security program includes “*security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency*.” Regarding training, FISMA directs agency heads to delegate to the CIO the authority to ensure compliance with information security requirements, including *“training and overseeing personnel with significant responsibilities for information security . . .”* FISMA goes on to task agency heads to *“ensure that the agency has trained personnel sufficient to assist the agency in complying with (FISMA) requirements.”* Clearly, FISMA intends organizations to identify those people who have significant responsibilities for information security and ensure they are trained to the level needed to perform their security-related tasks.

In June 2004, OPM issued a revision to the Federal personnel regulations. The changes build upon information technology awareness and training requirements contained in FISMA, and capture key concepts from NIST SP 800-50, “*Building an Information Technology Security Awareness and Training Program”* and NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training*”. This regulation, 5 Code of Federal Regulations (CFR) Part 930, Subpart C, is entitled “*Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems*” and requires Federal Organizations to provide training as set forth in NIST guidelines. Key requirements from the OPM regulation include:

* + - Develop an information technology awareness and training plan;
    - Identify employees with significant information technology responsibilities and provide role- specific training in accordance with NIST standards and guidelines;
    - Expose all users of Federal information systems to information technology awareness materials at least annually;
    - Provide training to the following groups:
      * Executives;
      * Program and functional managers;
      * CIOs, information technology program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers); and
      * IT function management and operations personnel;
    - Provide information technology awareness and training to all new employees before allowing them access to systems;
    - Provide information technology refresher training for agency employees as frequently as determined by the agency, based on the sensitivity of the information that the employees use or process; and
    - Provide training whenever there is a significant change in the agency information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

OMB Circular A-130, “*Management of Federal Information Resources,*” Appendix III, “*Security of Federal Automated Information Resources,*” also emphasizes these mandatory training requirements. Specifically, it requires that prior to being granted access to applications and systems, all individuals

must receive specialized training focusing on their information security responsibilities and established system rules.

## Relationships with Other NIST Documents

NIST SP 800-50, “*Building an Information Technology Security Awareness and Training Program,*” identifies the critical steps in the life cycle of an information security awareness and training program. Early in the life cycle of an agency’s awareness and training program an agency-wide Needs Assessment should be conducted. The results of the Needs Assessment should serve as the basis of an implementation strategy, which should be developed and then approved by the organization’s management. This strategic planning document identifies implementation tasks to be performed in support of established agency security training goals.

Federal Information Processing Standards (FIPS) 200, “*Minimum Security Requirements for Federal Information and Information Systems*,” introduces awareness and training as one of the seventeen areas (called “families” and does not include Program Management) of minimum security requirements identified to protect the confidentiality, integrity, and availability of Federal information systems and the information processed, stored, and transmitted by those systems.

NIST SP 800-53, “*Security and Privacy Controls for Federal Information Systems and Organzations,”* provides more detail to the awareness and training area identified in FIPS 200. This document provides levels for each control, dependent upon the system categorization and corresponding baseline. An information system will be classified at a low, moderate or high level. As the security controls change for each level so will the intensity of the training. Four specific controls in the Awareness and Training (AT) control family

include:

* + - AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

The organization develops, disseminates, and reviews/updates (organization defined) a formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entitles, and compliance; and formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

* + - AT-2 SECURITY AWARENESS TRAINING

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users; when required by information system changes; and (organization defined) thereafter.

* + - AT-3 ROLE-BASED SECURITY TRAINING

The organization provides role-based security training to information system users before authorizing access to the information systems or performing assigned duties; when required by information system changes; and (organization defined) thereafter.

* + - AT-4 SECURITY TRAINING RECORDS

The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for (organization defined).

Additionally, the Contingency Planning (CP) and Incident Response (IR) control families have specific controls addressing training:

* + - CP-3 CONTINGENCY TRAINING

The organization provides contingency training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties; when required by information system changes; and (organization defined) thereafter.

* + - IR-2 INCIDENT RESPONSE TRAINING

The organization provides incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties; when required by information system changes; and (organization defined) thereafter.

NIST SP 800-53A, *“Guide for Assessing the Security Controls in Federal Information Systems and Organizations,”* provides guidelines for the assessment of the effectiveness of implemented awareness and training controls within an organization. Security control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, security controls assessments are the principal vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives. This Special Publication is written to facilitate security control assessments conducted within an effective risk management framework. The assessment results provide organizational officials with:

* + - Evidence about the effectiveness of security controls in organizational information systems;
    - An indication of the quality of the risk management processes employed within the organization; and
    - Information about the strengths and weaknesses of information systems which are supporting organizational missions and business functions in a global environment of sophisticated and changing threats.

## Scope

This document describes IT/cybersecurity role-based training and its primary focus is to provide a comprehensive, yet flexible, training methodology for the development of role-based training courses or modules for personnel who have been identified as having significant IT/cybersecurity responsibilities within Federal Organizations. It should be noted that the trainer or training developer are not expected to be a SME in all functions but able to provide the appropriate training for a particular role.

Additionally, each Federal Organization can tailor the training to fit their specific roles.

## Audience

Management, from the highest to lowest levels, must understand the necessity of role-based training. Planning for the development, implementation and evaluation of role-based training within their organization is an essential function of management. All levels of management should understand how roles with security related responsibilities are identified within their organization. Management should

also be aware of those roles which will require the training as well as those who will develop the training. This publication should be read, reviewed, or understood by several key audiences to include the IT senior managers and leadership, management, SAISO, CISSO, ISSO, IAM, and PM and/or individuals required to understand based on the Federal Organization’s leadership structure. Target audience includes:

* + - IT/cybersecurity professionals that have responsibility for implementing the security role-based training portions of a Federal Organization’s IT/cybersecurity awareness and training program;
    - Federal IT/cybersecurity training personnel and their contractors tasked with designing role-based training courses or modules for Federal Organization’s personnel who have been identified as having significant responsibilities for IT/cybersecurity; and
    - Training developer/IDS tasked with developing and possibly delivering the awareness training and role-based training material and courses (or modules), may also use this document as guidance.

It is important to note that use of NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training,*” by the training developer and instructional designer is critical. Those who develop the training requirement and those who develop the training materials must use the same training methodology.

## Assumptions

Personnel identified as having significant responsibility for IT/cybersecurity should receive awareness training, as well as role-based training to address their additional responsibilities. NIST provides guidelines to assist with awareness presentations, awareness training and implementing security programs.

Personnel should have a base knowledge of cybersecurity essentials – familiarity, awareness, or understanding of security - from previous job experience, training, education (defined as “knowledge or skill obtained or developed by a learning process”), and their annual security awareness activity. With this annual security awareness and cybersecurity essential understanding, the following overall foundational competencies are assumed for the purpose of this document:

* + - Mathematics – a basic understanding of mathematics;
    - Organizational Awareness – a basic understanding of their organization and the threats/risks associated with it;
    - Quality Assurance – a program for the systematic monitoring and evaluation of the various aspects of a project to ensure that standards are being met;
    - Reasoning – solving a problem by considering various possible solutions;
    - Communications – basic writing and communication skills and an understanding of how to clearly communicate with peers;
    - Concepts – understands the basic intent of information assurance concepts;
    - Social Media – a basic understanding of the risks associated with the use of social media;
    - Ethics and ethical testing – conducts all evaluations and actions with approved methods and only on those systems allowed;
    - Teamwork - successfully work as a member of a team;
    - Task management – manage time according to a plan, complete tasks in a timely manner; and
    - Use of Information Technology tools—basic familiarity.

Personnel need to understand the basics of risk management, as defined in NIST SP 800-37, “*Guide for Applying the Risk Management Framework to Federal Information Systems*”. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, instructions, standards, and/or regulations.

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

**Security Life Cycle**



**ASSESS**

**Security Controls**

**IMPLEMENT**

**Security Controls**

**AUTHORIZE**

**Information System**

**MONITOR**

**Security Controls**

**SELECT**

**Security Controls**

**CATEGORIZE**

**Information System**

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

Figure 1.1 Risk Management Framework

The following activities related to managing organizational risk (also known as the Risk Management Framework – see figure 1.1) are paramount to an effective IT/cybersecurity program and can be applied to both new and legacy information systems within the context of the system development life cycle and the Federal Enterprise Architecture (specific guidance can be found in the NIST SP 800-37, “*Guide for Applying the Risk Management Framework to Federal Information Systems”*).

* + - **Step 1: Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis;
    - **Step 2: Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based

on organization assessment of risk and local conditions;

* + - **Step 3: Implement** the security controls and document how the controls are deployed within the information system and environment of operation;
    - **Step 4: Assess** the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;
    - **Step 5: Authorize** information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the information system and the decision that this risk is acceptable; and
    - **Step 6: Monitor** and assess selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials.

Lastly, this methodology assumes that the role-based training will be tailored to fit the Federal Organization’s identified roles and language.

## Document Organization

This guideline is divided into seven chapters and seven appendices.

* + - Chapter 1 (Introduction) describes the legislative and policy drivers, relationships with other NIST documents, purpose and scope, audience, assumptions and outlines the organization of this document;
    - Chapter 2 (Perspectives) describes the rationale, responsibilities and background needed to understand the training methodology;
    - Chapter 3 (Responsibilities) describes the learning continuum (e.g., IT/cybersecurity awareness, awareness training, specialized role-based training, and education), the model of the continuum and introduces the concept of role-based training;
    - Chapter 4 (Cybersecurity Continuum) describes the implementation of role-based training, development of training, explains the purposes of the appendices and the roles and responsibilities within an organization and its people;
    - Chapter 5 (Role-Based Training Methodology) provides a worked example of the methodology;
    - Chapter 6 (Worked Example) describes methods of evaluating the role-based training;
    - Chapter 7 (Training Evaluation) addresses methods to evaluate the effectiveness of training;
    - Appendix A (Functions) contains the functions within the organization and the desired Learning Objectives;
    - Appendix B (Knowledge and Skills Catalog) contains appropriate knowledge and skills for each knowledge unit;
    - Appendix C (Roles) contains roles and associated information;
    - Appendix D (Sample Evaluation Forms) contains recommendations for evaluating training effectiveness;
    - Appendix E (Glossary) provides the definition for the terms used throughout NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training*” ; and
    - Appendix F (Acronym) provides the acronyms and associated meaning.
    - Appendix G (References) provides references to National level guidance.

# Chapter 2 – Perspectives

Role-Based training is required by FISMA. FISMA metrics state that

*“successful performance in this area would require the organization to know the total inventory of persons needing training and the content of training needed based on each person’s role, the actual training provided and the user’s performance result (usually test results) ... and have a process to address the differences by providing training or removing access rights and responsibilities.”*

Furthermore, Role-Based training enhances an organization’s security posture through a trained workforce and it increases the individual’s readiness to respond to security incidents.

It is important to understand how the various government directives and guidelines interact with each other, and where the authority lies. FISMA is at the apex and represents the congressional mandate for Role-Based training. The FIPS are written as implementers, and these include FIPS 200 “*Minimum Security Requirements for Federal Information and Information Systems”* and FIPS 199 “*Standards for Security Categorization of Federal Information and Information Systems*”. Along with the FIPS, NIST SP 800-37 “*Guide for Applying the Risk Management Framework to Federal Information Systems”*, NIST SP 800-53 “*Security and Privacy Controls for Federal Information Systems and Organizations”*, NIST SP 800-18 “*Guide for Developing Security Plans for Federal Information Systems,”* and NIST SP 800-50 “*Building an Information Technology Security Awareness and Training Program”* provide additional guidance on how to meet FISMA requirements. These various documents provide the background, authority and additional resources to assist with the implementation of Role-Based training

The National Initiative for Cyber Education (NICE) has published a framework for the cyber workforce, including identifying various roles and functions. The National Cybersecurity Workforce Framework should be viewed as a bridge between human resources and the IT/cybersecurity departments. This bridge allows the Federal Government to have a view into the cyber workforce, and provides a framework on how to educate the workforce. This document (NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training* “) provides a *methodology* on how to train the personnel within the Federal workforce that have significant IT/cybersecurity responsibilities.

It is important to understand that there is a difference between Education and Training. The purpose of education is to provide learning and understanding of a subject; whereas the purpose of training is to ensure the individual can perform (doing) the functions required. For example, an aeronautical engineer is *educated* on the aerodynamics of an aircraft, and a pilot is *trained* on how to fly the aircraft.

Training should be focused on providing individuals with the skills necessary to fulfill security responsibilities and functions associated with their role; roles that may or may not be IT or IT security related. A role in this document is defined as the job function performed. A function is the action for which a person is specially trained. This document does not cover every role, but rather provides generic roles that can be tailored by the Federal Organization to meet their particular environment.

NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training”* also provides guidance on the methodology to develop IT/cybersecurity Role-Based training. This primary focus is to provide a comprehensive, yet flexible, training methodology for the development of Role-

Based training courses or modules for personnel who have been identified as having significant IT/cybersecurity responsibilities within Federal Organizations. It should be stressed that the Federal Organizations need to identify the roles within their specific organization; tailor the required or needed skills and knowledge to those roles, and ensure the training is developed with any specific organizational language. It should be noted that the trainer or training developer is not expected to be a SME in all functions but should be able to provide the appropriate training for a particular role.

This document introduces the concept of Cybersecurity Essentials training. There is a step (or gap) between the annual security awareness that is provided to all users, as a general introduction to good security practices, and the Role-Based training which is specific to the job functions. Role-Based training is built upon the Cybersecurity essentials. Cybersecurity essentials training includes computer basics and literacy, and could include fundamental computer skills, basic mathematical understanding and abilities that cannot be taught, such as teamwork. The Cybersecurity Essential training is further discussed in Chapter 4, the Learning Continuum.

Competencies are acquired when an individual gathers knowledge and hones skills in a certain functional area (Knowledge and Skills = Competencies). Certain roles require certain competencies, such as a security engineer requires analytical abilities to detect and identify network problems. This differs from proficiencies, which are acquired through experience and education. Proficiencies increase as the acquired competencies, associated skills and knowledge, are utilized over time.

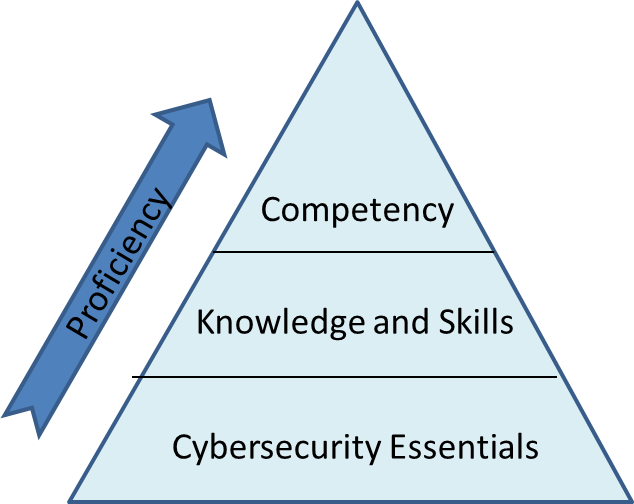


Figure 2.0 Cybersecurity Proficiency

It is critical to understand the difference between Security Awareness and Role-Based Training. Security Awareness provides individuals with awareness that there are good practices that will increase the organization’s security posture, but it is not considered functional or Role-Based Training. For example, security awareness is provided to all employees and contractors from the senior manager to the

administrative assistance. The awareness agenda may identify where to find security policies, that strong passwords are required or that you must wear your identification badge above the waist.

Role-Based training provides role-specific training for an individual based on their functional job and responsibilities. For example, Role-Based training for a network engineer will build upon the Cybersecurity Essentials and may include how to specifically set up the roles for the firewalls and the consequences if they are not set up properly. As a second example, Role-Based training for a senior manager may include understanding of the implementation of security controls, and the consequences if those controls are not implemented correctly.

There are functions and associated roles within some Federal Organizations that are very specific. Due to the sensitivity, uniqueness, and highly specialized nature of these roles, knowledge units and supplemental guidance are not provided for these specialty areas. However, those Federal Organizations with these roles can use the current knowledge and skills to develop appropriate role-based training.

The National Cybersecurity Workforce Framework provides insight into these specialty areas as part of the cyber workforce.

# Chapter 3 Organizational Responsibilities

While it is important to understand the policies that require Federal Organizations to develop IT/cybersecurity awareness training courses and role-based training courses or modules, it is crucial to understand who has responsibility for security training as well as those individuals who have significant security responsibilities and require the training. Personnel within Federal Organizations must understand who within their organization has the responsibility for identifying roles and developing role-based training materials.

## Organizational Responsibilities

An individual’s need for IT/cybersecurity training will change as their role changes. Within a particular role, over time, an individual’s responsibilities may change as they assume more management, acquisition, technical, or oversight responsibility. Some roles will have more management responsibility and less technical responsibility. Some roles will have more acquisition-related responsibilities and fewer management or technically-oriented responsibilities. Some roles will have more technical responsibilities and far less management responsibilities. Others will have more oversight responsibilities.

The training methodology described in this document is flexible to account for the various responsibilities found in a role, or across many roles. The Federal Organization should tailor the training to include all their IT or IT security related roles.

## Organization Head

Heads of Federal Organizations must ensure that high priority is given to effective role-based training for their workforce. This includes implementation of a viable IT/cybersecurity program with a strong awareness and training component. Agency heads should:

* + - Designate a Chief Information Officer;
    - Assign responsibility for IT/cybersecurity;
    - Ensure that an agency-wide IT/cybersecurity program is implemented;
    - Ensure resources and budgets are available to support the IT/cybersecurity program;
    - Measure the effectiveness of the IT/cybersecurity program; and
    - Ensure that the agency has sufficiently trained and will continue to train new personnel to protect its information resources.

## Chief Information Officer (CIO)

CIOs are tasked under FISMA to administer training and oversee personnel with significant IT/cybersecurity responsibilities. CIOs should work with the SAISO to:

* + - Establish the overall strategy for the IT/cybersecurity awareness and training program;
    - Ensure that the agency head, senior managers, system and information owners, and others understand the concepts and strategy of the IT/cybersecurity awareness and training program;
    - Report on the progress of the program’s implementation;
    - Ensure that the agency’s IT/cybersecurity awareness and training program is funded;
    - Ensure the training of agency personnel with significant IT/cybersecurity responsibilities;
    - Ensure that all users of information systems are sufficiently trained in their security responsibilities;
    - Ensure all users receive security awareness training; and
    - Ensure that effective tracking and reporting mechanisms are in place for all facets of training.

## Senior Agency Information Security Officer (SAISO)

The SAISO has tactical-level responsibility for the organization’s IT/cybersecurity awareness and training program. In this role, the SAISO should:

* + - Ensure that role-based training material is appropriately developed and delivered in a timely manner for the intended audiences;
    - Ensure that role-based training material is effectively deployed to reach the intended audiences;
    - Provide an effective mechanism for feedback on role-based training security material and its presentation;
    - Ensure that role-based training material is reviewed periodically and updated when necessary; and
    - Assist in establishing a tracking and reporting strategy for training.

## Cybersecurity Training Manager/Chief Learning Officer (CLO)

The Cybersecurity Training Manager/CLO has the responsibility for the specific role-based training within the IT fields. This individual may or may not be a separate responsibility within the Federal Organizations:

* + - Ensure that role-based raining material is appropriately developed and delivered in a timely manner for the intended audiences;
    - Ensure that role-based training material is effectively deployed to reach the intended audiences;
    - Provide an effective mechanism for feedback on role-based training security material and its presentation;
    - Ensure that role-based training material is reviewed periodically and updated when necessary; and
    - Assist in establishing a tracking and reporting strategy for training.

## Managers

Managers at all levels, from the most senior to the most junior managers have responsibility for complying with IT/cybersecurity role-based training requirements established for their employees, users, and those who have been identified as having significant IT/cybersecurity responsibilities. Managers should:

* + - Work with the CIO and SAISO to meet shared responsibilities and emphasize the importance of IT/cybersecurity role-based training to the workforce;
    - Serve in the role of system owner and/or information owner, where applicable;
    - Consider developing Individual Development Plans (IDPs) for those with significant

IT/cybersecurity responsibilities;

* + - Ensure that all users (including contractors) of their systems and applications are appropriately trained in how to fulfill their IT/cybersecurity responsibilities prior to allowing them access;
    - Ensure that users (including contractors) understand specific rules of behavior for each system and application they use;
    - Work to reduce errors and omissions by users due to lack of specialized role-based training; and
    - Track all training progression and documented record training provided to employees.

## Training Developer/Instructional Design Specialists

Training Developers/IDSs, whether internal to an organization or external, are key players in an IT/cybersecurity awareness and training program. An organization usually requires the assistance of IDSs for the development of role-based training materials. IDSs should:

* + - Work with an IT/cybersecurity subject matter expert when developing role-based training material and courses to ensure that the proper material is included and is developed to the proper knowledge level for the audience; and
    - Understand the role-based training methodology in NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training”* since it is used to develop specialized courses or modules for those individuals who have been identified as having significant responsibilities for IT/cybersecurity.

## Personnel with Significant IT/ Cybersecurity Responsibilities

FISMA requires Federal Organizations to identify and train those personnel with significant IT/cybersecurity responsibilities. These personnel - whether executives, IT/cybersecurity program staff members, or system/network administrators - are in positions that are responsible for the security of the organization’s information and information systems. Because of their positions, they can have the greatest positive or negative impact on the confidentiality, integrity, and/or availability of Federal Organization information and information systems. These personnel must:

* + - Attend role-based training identified/approved by their management;
    - Advise their management of additional training that can help them better secure information and information systems for which they are responsible;
    - Understand that IT/cybersecurity is an integral part of their job;
    - Understand the organization’s expectations of their position;
    - Understand how to implement and maintain IT/cybersecurity controls;
    - Understand how to mitigate risk to information and information systems;
    - Monitor the security condition of the security program, system, application, or information for which they are responsible;
    - Respond appropriately when security breaches are discovered;
    - Apply what is learned during role-based training; and
    - Document and record all training received.

## Users

Users are the single most important group of people who can help reduce unintentional errors and related information system vulnerabilities. Users may include employees, contractors, foreign or domestic guest researchers, other organization personnel, visitors, guests, and other collaborators or associates requiring access to information and/or systems. Users must:

* + - Understand and comply with Federal Organization and Agency IT/cybersecurity policies and procedures; and
    - Be appropriately trained in the rules of behavior for the systems and applications to which they have access.

# Chapter 4 – Cybersecurity Learning Continuum

To successfully fulfill their roles within an organization, individuals must be given the right tools and training. The right tools and training include a combination of basic security awareness, essential skills, cooperative learning or on-the-job training, education, experience and the knowledge, skills and ability suited to the role. The Cybersecurity Learning Continuum assists in providing an approach to affording all the necessary information for individuals.

The objectives of learning are designed to permit a consistent, government-wide approach to ensure that all employees who are involved with IT systems, information technology, and cybersecurity activities - regardless of Agency, role, function, job or system – acquire the same, comprehensive understanding and training in security. The value of a consistent training program is the portability of Cybersecurity Essentials as employees change jobs and organizations.

Learning is a continuum; it starts with awareness, builds to training, and evolves into education. The Cybersecurity Learning Continuum provides context and the relationship between Security Awareness, Cybersecurity Essentials, Training and Education. The Learning Continuum demonstrates that Awareness and Cybersecurity Essentials form the fundamental baseline required for all individuals involved with the management, operation, maintenance, development or use of IT systems, information technology and cybersecurity. It also demonstrates that the training and education levels are more selective, based on a role and responsibility.

The Cybersecurity Learning Continuum, shown in Figure 4-1, is a progression of learning across the spectrum of roles within an organization. Security awareness training is provided to all users within an organization. Cybersecurity Essentials training is provided to all users involved with IT systems. Role- based training is provided to users with responsibilities relative to IT systems. Knowledge, education and/or experience are gained by IT Security Specialists and professionals. The appropriate level of cybersecurity awareness, training and education is determined by the role within an organization.

Individuals obtain skills as they participate in role-based training with their agency.

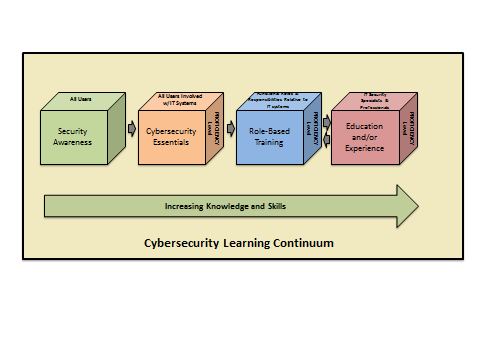


Figure 4-1: Cybersecurity Learning Continuum

The Cybersecurity Learning Continuum is designed to assist in demonstrating the level of training and awareness required for roles within an organization. NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training”* uses generic roles and job titles that may or may not be the same as the roles or job titles used by an individual Federal Organization. The roles and titles used within this document are a sample of current jobs/roles within various Federal Organizations and organizations at the time of publication. Here is an example to help identify roles, responsibilities and training needs:

Pearson is currently a system administrator within a Federal Organization. As an employee of a Federal Organization, Pearson must receive the annual security awareness training. He is also in the Information Technology Department, so he receives additional education on cybersecurity, known as Cybersecurity Essentials. In his role as system administrator, Pearson has significant IT responsibilities, and therefore, is also required to attend role-based training.

Polly, a college intern working as the office administrator for the summer, is required to take security awareness training. However, since her responsibilities are not significantly security based, she is not required to take any role-based training. But she may have gained some cybersecurity essentials knowledge from her course work or on-the-job experiences.

This chapter provides a brief overview of the Cybersecurity Learning Continuum and its application within the computer security arena. The learning continuum is referenced in various NIST Special Publications such as NIST SP 800-100, “*Information Security Handbook: A Guide for Managers”* and NIST SP 800-50, “*Building an Information Technology Security Awareness and Training Program”*. A model of the Cybersecurity Learning Continuum is shown in Figure 4-1. Although the curriculum provides a generic outline for material, each organization must keep in mind that it needs to relate and be tailored to their unique culture and mission requirements.

The curriculum was developed to present topics and concepts in a logical order, based on IT system planning and life cycle stages, but may be presented in any order. However, before it can be expected that an individual will be able to understand all aspects of security related to a particular role, some exposure to basic security should have been completed. The material presented is an introduction of the concepts and topics only, and these will be further expanded and enhanced at the role-based training level.

The model presented as Figure 4-1 is based on the premise that learning is a continuum. Learning occurs over a broad range of levels and topics. Specifically, learning in this context starts with awareness, builds to training, and evolves into education. This model provides the context for understanding and using this document, and identifying how role-based training interacts with other types of training.

The Cybersecurity Learning Continuum demonstrates that awareness and training form the baseline that is necessary for all individuals involved with the management, development, maintenance, and/or use of IT systems. It also demonstrates that role-based training and education are to be provided selectively, based on individual responsibilities and needs. Specifically, IT/cybersecurity training is to be provided to individuals based on their particular roles and IT/cybersecurity responsibilities, especially if they have been identified as having significant IT/cybersecurity responsibilities. IT/cybersecurity-focused education is intended for designated IT/cybersecurity professionals in addition to role-based training.

The Cybersecurity Learning Continuum provides the various types of learning. The type of learning that individuals need becomes more comprehensive and detailed at the top of the continuum. Thus, beginning at the left, all employees need to be exposed to awareness. All information system users need awareness training. Specialized training is required for individuals whose role in the organization indicates a need for special knowledge of IT/cybersecurity threats, vulnerabilities, and safeguards. The “Education” phase of the model applies primarily to individuals who have made IT/cybersecurity their profession.

The model illustrates the following concepts:

* “Security Awareness” is explicitly required for all employees. In today’s environment this typically means all individuals within the organization;
* “Cybersecurity Essentials” is needed for those employees, including contractor employees, who are involved in any way with IT systems. Cybersecurity Essentials is the transitional stage between “Basic Awareness” and “Role-Based Training.” It provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts;
* “Role-Based Training” becomes focused on providing the knowledge and skills specific to an individual’s roles and responsibilities relative to Federal Organization information systems. Their role within the organization is primary with IT secondary. Decision responsibilities come from the organization role, whereas the technical responsibilities are derived from the relationship with

IT. At this level, training recognizes the differences between competencies among the trainees; and

* “Education” focuses on developing the ability and vision to perform complex multi-disciplinary activities and the skills needed to further the IT/cybersecurity profession and to keep pace with threats and technology changes. This can be accomplished with experience, cooperative training such as “on the job” training or through certification and advanced education such as undergraduate and graduate studies and degrees as accepted by the particular Federal Organization.

Learning is a continuum in terms of levels of knowledge, but the acquisition or delivery of that knowledge need not proceed sequentially. Given resource constraints, organizations have a responsibility to evaluate against the continuum both the scope of their IT/cybersecurity training needs and the effectiveness of the training provided. This enables an organization to be able to allocate future training resources to derive the greatest value or return on investment.

## Security Awareness

The subject of developing IT/cybersecurity awareness material is discussed in NIST SP 800-50, “*Building an Information Technology Security Awareness and Training Program*”. The document is a companion publication to NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training”.* The two publications are complementary – NIST SP 800-50, “*Building an Information Technology Security Awareness and Training Program”* works at a higher strategic level, discussing how to build an IT security awareness and training program, while NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training*” is at a lower tactical level, describing an approach to role-based IT cybersecurity training.

The purpose of Security Awareness is to focus attention on and establish recognition of security and security issues. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.

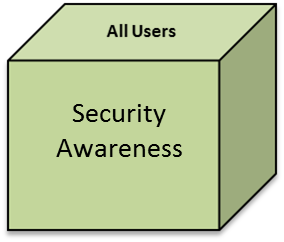


Figure 4-2 Security Awareness

Security awareness is a blended solution of activities that promote security, establish accountability, and inform the workforce of security news. Awareness seeks to focus an individual’s attention on one issue or a set of issues. Awareness activities are intended to allow individuals to recognize IT/cybersecurity concerns and respond accordingly.

In awareness activities the learner is a recipient of information. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate job performance.

Learning achieved through awareness activity alone tends to be short-term, immediate, and issue-specific. For example, if a learning objective is “to facilitate the increased use of effective password protection among employees,” an awareness activity might be the use of reminder stickers for computer keyboards or global emails to all employees emphasizing the use of effective passwords.

Awareness also strives to build in an organization’s information system user population foundation of IT/cybersecurity terms and concepts upon which later role-based training, if required, can be based.

Awareness informs users of the threats and vulnerabilities that impact their organization and personal work environments by explaining the “what” but not the “how” of security, and communicating what is and what is not allowed. Security Awareness not only communicates IT/cybersecurity policies and procedures that need to be followed, but also provides the foundation for any sanctions and disciplinary actions imposed for noncompliance. Security Awareness is used to explain the rules of behavior for using an organization’s information systems and information and establishes a level of expectation on the acceptable use of the information and information systems.

The fundamental value of Security Awareness programs is that they set the stage for role-based training by bringing about a change in attitudes which should begin to change the organizational culture, which better secures the Federal organization’s mission through more secure systems. The cultural change sought is the realization that IT/cybersecurity is critical because a security failure has potentially adverse consequences for everyone. IT/cybersecurity is everyone’s job. Detailed guidance on IT/cybersecurity awareness is outside the scope of NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training*” but is covered in more depth in NIST SP 800-50 “*Building an Information Technology Security Awareness and Training Program*”.

In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.

## Cybersecurity Essentials

The Cybersecurity Essentials level on the Cybersecurity Learning Continuum is the transition between Security Awareness and Role-Based training. This level is the foundation for further specific learning related to one’s role(s) with respect to IT systems. This foundation is required before the individual can move forward in their learning. Training may be tailored to a specific organization’s IT environment, security policies, and risks.

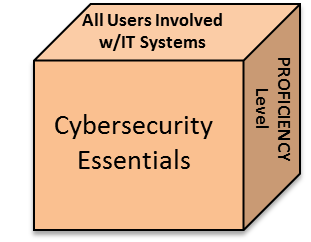


Figure 4-3 Cybersecurity Essentials

Cybersecurity Essentials, in addition to knowledge gathered via security awareness, provide a general introduction to security. FISMA requires those individuals with significant IT/cybersecurity responsibilities have role-based training. The transition from security awareness to role-based training takes place beyond the security basics and cybersecurity essentials level.

While NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training”* concentrates on role-based training, there is an assumption that the individual has security basics knowledge. IT/cybersecurity knowledge grows commensurate with today’s rapidly technology changes. Regardless of its size and growth rate, there are certain basic concepts that form the foundation of any effective IT security program and environment. These terms and concepts must be learned and applied as the individual proceeds from security awareness to training and then to education and experience.

The Cybersecurity Essentials are necessary to provide an individual with a slightly increased level of security material which allows for the development or evolution of a more robust awareness program. It may also provide the foundation for the training program.

Cybersecurity Essentials must not be confused with computer literacy, as the latter refers to an individual’s familiarity with a basic set of knowledge that is needed to use and maintain a computer. Cybersecurity Essentials refers to an individual’s familiarity with – and ability to apply – a core knowledge set which is needed to protect electronic information and systems. Cybersecurity Essentials is not geared to any specific system but rather is the foundation for further learning. All individuals who use computer technology or its output products, regardless of their specific job responsibilities, must know these essentials and be able to apply them.

The Cybersecurity Essentials level key terms, essential concepts and principles include an understanding of:

* Technical underpinnings of cybersecurity and its taxonomy, terminology and challenges;
* Common information and computer system security vulnerabilities;
* Common cyber attack mechanisms, their consequences and motivation for use;
* Different types of cryptographic algorithms;
* Intrusion, types of intruders, techniques and motivation;
* Firewalls and other means of intrusion prevention;
* Vulnerabilities unique to virtual computing environments;
* Social engineering and its implications to cybersecurity; and
* Fundamental security design principles and their role in limiting point of vulnerability.

## Role-Based Training

Roles are established by the Federal Organizations through positions, position descriptions, hierarchy charts, responsibilities, etc. These show how the work required to achieve a particular objective have been identified. Individuals may assume additional roles based on their individual skills, organization policies regarding cross-training and backup, and organizational staffing levels. Some examples of roles include: network administrator, system administrator, information assurance technician, information assurance manager, cybersecurity technician, cybersecurity manager, Computer Information Security Officer (CISO), CIO etc. This is just a sampling of the many roles in the IT/cybersecurity arena and may not reflect the roles within a particular Federal Organization. The roles may be tailored to reflect the Federal Organizations environment.

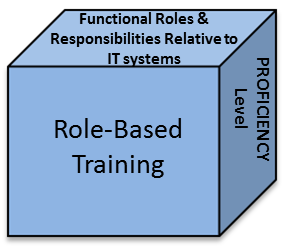


Figure 4-4 Role-Based Training

Training is more formal, is structured and has a goal of building knowledge and skills to facilitate the job performance. Whereas, the purpose of awareness presentations is to focus attention on security.

The cybersecurity learning continuum model is role-based and defines the IT/cybersecurity learning needed as a person assumes different roles within an organization and different responsibilities in relation to information systems. In other words, role-based training teaches a certain skill based on the assigned role and identifies the expected knowledge, skills and competencies from the training. Training strives to produce relevant and needed security skills and competencies. This document uses the model to identify the knowledge and skills an individual needs to perform the IT/cybersecurity responsibilities specific to each of his or her roles in the organization.

IT/cybersecurity role-based training strives to produce relevant and needed security knowledge and skills within the workforce, specifically, in those individuals identified by their organization as having significant responsibilities for IT/cybersecurity. Role-based training supports competency development and helps personnel understand and learn how to better perform their specific security role, which ultimately better secures the Federal Organization’s mission through more secure and protected information and systems. The most important difference between training and security awareness is that awareness is intended to make the individual recognize that there is a problem and react. Training allows that individual to react, develop and implement a proper response to the problem.

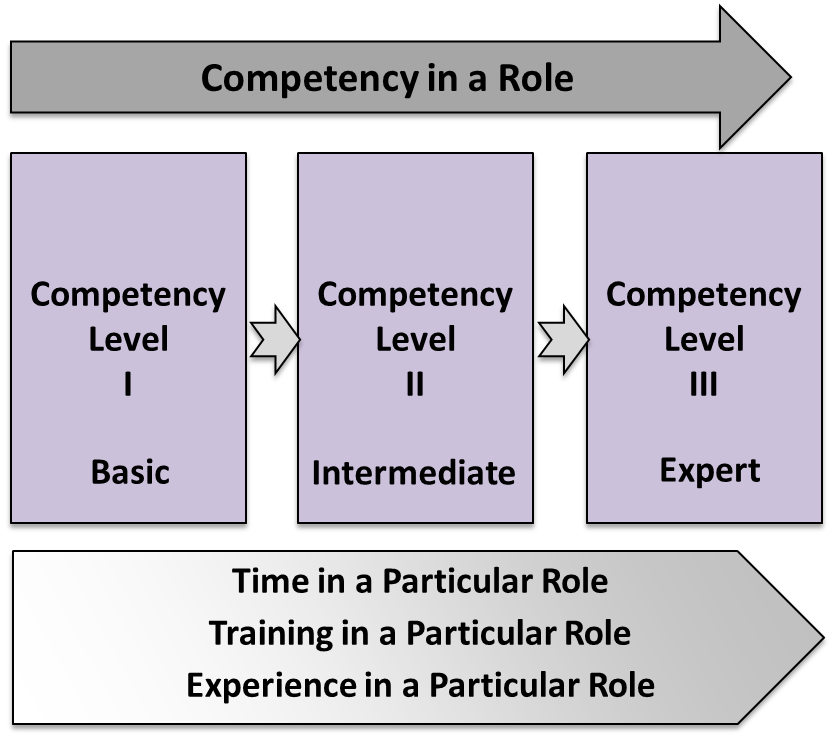
Role-based training is required for any individual who has influence over an information system, application or network; the information; and/or organization mission. Obvious roles are the system administrator or the system developer. Less obvious roles are the program manager or procurement officer, who also needs to understand the security implications of their decision, actions or purchases. Regardless, each role has certain skills associated with that role; and that knowledge and associated skills must be taught.

Roles are not simply job titles, although a role may be associated with a job title. Roles may be job titles or functions, and are called out differently in each agency. Whatever the role is called, there are associated competencies, knowledge and skills which must be learned by the individual who occupy that role. A role-based training curriculum may not necessarily lead to a formal degree from an institution of higher learning; however, a role-based training course may contain much of the same material found in a course that a college or university includes in a certificate or degree program.

**Competency Levels**

For illustrative purposes in this document three competency levels are described. These levels may not relate to skill or experience levels used by a particular organization. Figure 4-5 provides a visual of this concept.

* Competency Level I skill requirements are basic and are usually obtained during the first few years in that role. Although a person may have been working in the security arena for the last 15 years, if they move into a new role requiring additional functional skills they would need to possess more than Competency level I skills;
* Competency Level II skill requirements are considered intermediate, and are those skills that have obtained and honed during more years in that role; and
* Competency Level III skill requirements are considered expert, and are those skills that can only be obtained after many years in the role.



33

Figure 4-5, Competency Levels

Over time, individuals acquire different roles relative to their use of information and information systems and applications within their organization or as they move within various Federal Organizations. Roles can expand or change as an individual progresses through their career, either within one organization, or as they make career moves to different organizations. Sometimes they will be users of systems and applications; in other instances they may be involved in developing a new system; and in some situations they may serve on a source selection board to evaluate vendor proposals for information systems. The IT/cybersecurity responsibilities that an individual has will also change over time, and will correlate to the role that the individual has, relative to information and information systems and applications. Training must be available – whether developed within the organization, borrowed or purchased from another organization, or developed by a training company – for people in each role who have been identified as having significant IT/cybersecurity responsibilities.

Here is an example of how an individual may have multiple roles during his/her career:

Pearson has been in the IT field his entire career and has had multiple roles. He started his career as a technician on the call desk, and as such, would have been trained in that role. After a few years, he moved into a system administrator position, which required more knowledge and skills. At year 12 in his career, he changed organizations and became a team lead. This required him not only to receive training in the functional perspective of management, but also required him to learn organization specific requirements. He finally ended his career as a Senior Network Administrator. As you can see, Pearson had various roles within his career and these roles require role-based training for those various positions.

The roles listed and described in NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training*” carry varying degrees of responsibility for IT/cybersecurity, depending on what particular work an organization assigns to each role. Therefore, the person serving in one role will likely have more or less information/cybersecurity responsibility than will a person serving in another role and will need to know more about some aspects of IT/cybersecurity than will a person serving in another role. For example, a CIO or SAISO/CISSO will need to know more about Federal laws and regulations and Agency policy than will a system administrator. They will need to know more about managing an IT/cybersecurity program, while the system administrator will need to know far more about implementing and monitoring system-level controls, and usually far less about program management.

This is why this document focuses first on roles, then on what fundamental perspective the individual has and lastly, how much experience the individual has in that particular role. All of these aspects should be considered to be included in a training course or module for each role.

There are roles within some Federal Organizations that are very specific. These can include roles, such as Collection Operations, Cyber Operations Planning, Threat and Exploitation Analysis, All-Source Intelligence and Target Operations, as identified within the Cybersecurity Workforce Framework. Due to the sensitivity, uniqueness, and highly specialized nature of these roles, knowledge units and supplemental guidance are not provided for these specialty areas. However, those Federal Organizations with these roles can use the current knowledge and skills to develop appropriate role-based training.

The role-based training methodology is described in Chapter 5.

## Education and Experience

The Education level of the Cybersecurity Learning Continuum represents the additional option that both current and prospective IT/cybersecurity professionals have to build or enhance their security-oriented knowledge and skills.

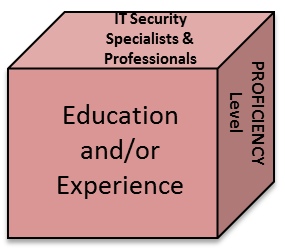


Figure 4-5 Education and/or Experience

While many IT/cybersecurity professionals enter the workforce with a formal education foundation, “education” as used within the Learning Continuum is meant to address the additional formal IT/cybersecurity –focused education that can be obtained to augment training and experience.

Education can include industry-recognized IT security certification as well as programs that are offered by higher education institutions.

To reach the advanced level of IT/cybersecurity professionalization, completion of formal education in the field is often required. This professionalization integrates training, education, and experience with an assessment mechanism to validate knowledge and skills, resulting in the “certification” of a predefined level of competence. The movement toward professionalization within the IT/cybersecurity field can be seen among IT/cybersecurity officers, IT/cybersecurity auditors, information technology contractors, and system/network administrators, and is evolving. An example of education that leads to professionalization is a degree program or certification program.

IT security education/professionalism criteria are outside the scope of this document.

## Role-Based Training Differs From Other Types of Training

While the phrase “role-based training” is used extensively to describe the training that should be provided to people who have significant responsibility for IT/cybersecurity; role-based training may also be called “formal training,” “specialized training,” or “functional training” in some organizations. All of these phrases are in contrast to Cybersecurity Essentials, which is the foundation of IT/cybersecurity knowledge, upon which the additional role-based training is built.

Topic-based training is training that is developed for a large group of individuals and covers a generic area; whereas role-based training allows the recipient of training to learn what he or she needs to know and be able to implement the knowledge, based on their current roles. This is perhaps the most important distinction between role-based and topic-based training. Topic based training, for example, is training on the Time and Attendance system whereas the learning objectives for every employee is the same. While topic-based training is easier to develop because, for the most part, it can be developed once and for diverse audiences, it approaches being a one-size-fits-all solution. Unfortunately, an easy solution like this to a complex issue like IT/cybersecurity training can, in itself, be considered as a vulnerability as dangerous as a poorly configured operating system or firewall. Recipients of topic-based training, for the most part, must interpret what they see and hear during a training session, determining what it is that they need to learn and be able to do and what does not apply to them, based on their role.

Typically, material included in a topic-based training course is meant to be consumed by people who fill a number of different roles. For example, “generalists” – those attendees in many management-oriented roles – who need to understand some information about many different topics are likely going to be overloaded with details about topics about which they need to know little. Conversely, “specialists” – those attendees in many technical roles – who need to be exposed to relatively fewer topics, but must understand these topics in far greater depth, are more than likely going to be disappointed when those topics are not adequately addressed, therefore, the training will not meet their needs. As a result, role- based training - which tailors the training to the role, functional perspective and experience – is required within the security arena.

Throughout their career, individuals acquire different roles relative to the use of IT systems and information within an organization, or as they transition to other organizations. In these various roles, they may be a user, administrator, manager or developer. They could even have the roles of a source- selection team for a new IT system, or developing the budget to maintain the IT system and as such, its security baseline. Therefore, the needs for training change as the roles change. To address this change, the role-based training has been segmented into categories of functional perspectives:

* + - Manage – the individual’s job functions encompass overseeing a program or technical aspect of a security program; overseeing the lifecycle of a computer system, network or application; or have responsibilities for the training of staff;
    - Design – the individual’s job functions encompass scoping a program or developing procedures, process and architectures; or design of a computer system, network or application;
    - Implement – the individual’s functions encompass putting programs, processes, polices into place; or operation/maintenance of a computer system, network or application; and
    - Evaluate – the individual’s functions encompass assessing the effectiveness of any of the above actions.

These functional perspectives will be further explained in Chapter 5.

Within each of these areas, the trainer should tailor the knowledge and skills to address the individual’s role and competency. That is, are they relatively new to the area – such as becoming a team lead from an administrator position? Or are they very experienced from having been in that role for years?

The tailoring process allows the organization to modify the roles appropriately and align the training more closely with the specific training needs for the organization as well as per the individual trainee. The tailoring process includes:

* + - * Identifying the needs of the organization/individual trainee (e.g., skills, knowledge and competency);
      * Applying scoping considerations to the training modules;
      * Selecting or developing training modules;
      * Supplementing training, if needed; and
      * Providing additional specification information, if needed.

Ultimately, organizations use the tailoring process to achieve cost-effective, risk-based security that supports organizational mission/business needs. This includes the training of their employees. Tailoring activities are approved by authorizing officials in coordination with the CLO prior to implementation.

Organizations have the flexibility to perform the tailoring process at the organization level for all role- based training.

# Chapter 5 – Role-Based Training Methodology

## Role-Based Training

As previously discussed, the role-based training level includes the security-related experience as well as the specific area the individual occupies. Functional perspectives are also helpful to identify and scope requirements for each role and enhance the training development and outcomes. For the purposes role- based training, the following specific functional perspectives are generically 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; including the management of any program, persons, or operations;
    - **Design:** Functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level; as well as the secure development of systems, networks or applications;
    - **Implement:** Functions that encompass putting programs, processes, or policies into action within an organization; including operation and maintenance of systems, networks or applications; and
    - **Evaluate:** Functions that encompass assessing the effectiveness of a program, policy, process, or security service in achieving its objectives; including the evaluation of the security state of a system, network or application.

In addition to the functional perspectives, the amount of experience the individual possesses needs to be considered when providing role-based training. Experience/proficiency or competency levels are defined by each Federal Organization.

All of these areas are used to tailor the training to the specific role.

To further explain the importance of functional perspective, we will revisit “Pearson” as an example to show how the area and competency level works.

Pearson has been in the IT field his entire career. He started his career as a technician on the call desk, and as such, would have been trained in this role. For this role, the training module would have to cover those requirements in “implement” at Competency Level I. After a few years, he moved into a system administrator position, which required more knowledge and skills. His training requirements in this position were functionally aligned with either “implement” or “evaluate” and his competency was at Competency Level II since some of the experience he acquired as a technician can be applied to his system administrator position. At year 12 in his career, he changed organizations and became a team lead. He was then trained for his functional role to “manage” and returned to a Competency Level I since this is a new area for him. He finally ended his career as a Senior Network Administrator - we will assume that Pearson had at least 10 years in this role so he would be trained to “implement” and is now at Competency Level III.

## Developing and Implementing Role-Based Training

The SAISO, IT/cybersecurity program managers and staff, and auditors should also be familiar with the scope of this document, and should understand the applicability of role-based courses or modules for those who have been identified as having significant responsibilities for IT/cybersecurity. The SAISOs and other IT/cybersecurity practitioners should use NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training*” to determine at which point they hand over responsibility for material development to training developers/IDSs.

Both the CIO and SAISO should understand that the role-based training builds upon the Cybersecurity Essentials. Additionally they should understand that the Cybersecurity Essentials is not the same as the security awareness training, but rather the bridge between the basic understanding and the specific training.

NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training*” concentrates on the role-based IT/cybersecurity training. Personnel will need to work together to meet their responsibilities which include, but not limited to:

* + - Management: All levels of management will be responsible for their staff training needs; prioritize the use of training resources, identify training gaps and evaluate the training effectiveness;
    - IT/Cybersecurity Specialist: The IT/Cybersecurity specialist will be responsible for assisting in the identification of one (1) the requirements of the roles or job functions; two (2) training gaps and needs within the organization’s IT/Cybersecurity program; three (3) customization that is needed and four (4) a compliance baseline for the organization; and
    - Training Professionals: This group includes human resource planners, training coordinators/curriculum developers, course developers/IDSs, and, of course the trainers

responsible for developing, presenting and evaluating the training. NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training*” will assist the training profession in understanding the IT security knowledge/skills required; evaluate the course quality; obtain the appropriate courses and materials; develop or customize courses/materials; and tailor their teaching approach to achieve the desired Learning Objectives.

The training methodology described in this chapter focuses on providing the training developer/IDS or course developer, with the tools to build a course or module based on the IT/cybersecurity role of the intended audience. Additionally, the National Initiative for Cybersecurity Education (NICE) serves as a national resource for government, industry, academia, and the general public in their quest to learn about cybersecurity awareness, education, careers, and workforce development opportunities and can be used in identifying the organization’s workforce.

#### Agency-wide Needs Assessment, Job Task Analysis and Criteria

Before any training should be created, a Federal Organization should identify their training requirements, tasks and criteria that need to be met. Having this fundamental information ensures the training is targeted to meet the Federal Organization’s mission and IT/cybersecurity needs, and addresses the variety of roles within the Federal Organization. It is suggested the Federal Organization role-based security training be based on the results of a Federal Organization-wide Needs Assessments, which should identify any role-based training requirements. This chapter describes, at a high level, the steps to develop the role- based training.

#### Agency-wide Needs Assessment

The Agency-wide Needs Assessment will identify the relationship between identified role-based training requirements and an organization’s current efforts. The Needs Assessment helps identify these additional needs – the gap between what is currently being done and what is required. This should be completed prior to the development of training modules.

An Agency-wide Needs Assessment is helpful in beginning to establish and depict the training requirement for an organization. Conducting the Needs Assessment will assist in identifying any gaps in the organization’s current role-based training program, as well as any gaps in the current role-based training. Management must identify the skills required to perform the functions they assigned to specific Federal Organization roles. The role requirements are then analyzed to identify the learning required to acquire those skills and how it is expected to be acquired (formal training, On-the-Job Training (OJT), etc.). The focus of NIST SP 800-16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training*” is to develop the role-based training, not to conduct the Needs Assessment. The method of conducting a Needs Assessment is covered in NIST SP, 800-50, “*Building an Information Technology Security Awareness and Training Program”*. Additionally, NICE can be used as a resource for determining the organizations required workforce and the current gaps.

Another important result of the Needs Assessment is the related IT/cybersecurity role-based training program requirements. For example, if role-based training material will be presented utilizing Computer-Based Training (CBT) technology, a technical assessment should be conducted on the organization’s processing platform (e.g., local area network, workstations, video cards, speakers) to determine if the existing environment will support the new or expanded training program.

#### Job Task Analysis and Criteria

Although various organizations may use the same role name to describe or label people who do similar work, the actual knowledge and skills needed by incumbents in same-titled positions may vary from organization to organization, and even within the same Agency. A job task analysis that focuses on work currently being accomplished by people in the same role, or perhaps more accurately, doing what is perceived to be the same work, will highlight what training is needed, or how existing training courses or modules should be modified to meet employee needs.

There may be instances in which some people in a role, but not all, are identified as having significant IT/cybersecurity responsibilities. Depending on the criteria that an organization uses to make this determination – e.g., impact level of associated information, information system, or application; position sensitivity identified in position descriptions; significant IT/cybersecurity responsibilities identified in performance plans; specific personnel named in system security plans – some members of a role may be selected for training, while others who do not meet the organization’s criteria may not be required to attend the training. While these personnel may not be required to attend the role-based training designed for those with significant IT/cybersecurity responsibilities, their supervisors will likely insist that they receive some training - role-based or topic-based – even the same training as others in the same role.

#### Development Training Overview

After identifying the roles that require training, or any gaps in the current training, the development of the training modules can be completed. The appendices in this document can assist with ensuring that the training meets the requirements of the role.

“Scoping guidance” was first used in NIST SP 800-53, *“Security and Privacy Controls for Federal Information Systems and Organizations”*. Here, in the context of role-based training, “scoping guidance” is used to describe the flexibility an organization has to build, or have built, IT/cybersecurity courses or modules, using the results of Needs Assessments, job task analyses, and the training methodology described in this chapter. It is recommended that the organization scope the development of the training to meet the roles of their particular organization, and use the terminology that is understood by their employees.

The identification of a role or roles in need of training would be accomplished by: one (1) a Needs Assessment, two (2) an inspector’s review, or three (3) the person or people in the organization tasked with identifying those with significant IT/cybersecurity responsibilities. These processes can also identify whether training is to be developed where none exists for a role o r roles, or if existing training needs to be updated or modified. Regardless of how roles are identified for IT/cybersecurity training within an organization, supervisors remain the best barometer of individual training needs. Using position descriptions, performance plans, and individual development plans, supervisors - with input from their staff - can identify training needs. By coordinating with the organization’s IT/cybersecurity training function, supervisors can determine if the needed training is available in-house, or must be sought elsewhere.

Various methods to develop training are available to the Training Developer/IDS. The developer should ensure that the complexity of the training is commensurate with the role and the needs of the person or people who will undergo the learning effort. Material should be developed based on two important

criteria: one (1) the role, and two (2) knowledge and skills identified for that position.

When developing the training, keep in mind these key steps:

* Write an explanation of expected core skills to be learned. This is an overview of what class participants can expect to learn after progressing through the training materials;
* Establish learning objectives in accordance with the organizational mission;
* Dedicate a separate section to each learning objective;
* Create individual lessons for each of the learning objectives; and
* Integrate visual elements; use graphics, videos, tables and other visual tools to reinforce important concepts.

Training can be developed via various methods, which could include but are certainly not limited to: the systematic instructional design model consisting of five phases: (1) Analysis, (2) Design, (3) Development, (4) Implementation, and (5) Evaluation (known as ADDIE), Dick and Carey Systems Approach, Instructional Development Learning System (IDLS), and Kemp. In addition to various development methodologies, there are various training methodologies. These could include, but are not limited to: computer based training, classroom training, on-line courses and on-the-job training.

Training must be developed and provided if no such training exists for a role, and/or if the organization has identified that role as having significant IT/cybersecurity responsibilities.

Appendix A provides functions that may require role-based training. Specifically, Appendix A provides:

* + Function Areas;
  + Roles Areas - these roles are guidance and may exist under different names within a particular Agency;
  + Definitions of the functions; and
  + Learning Objectives of the training.

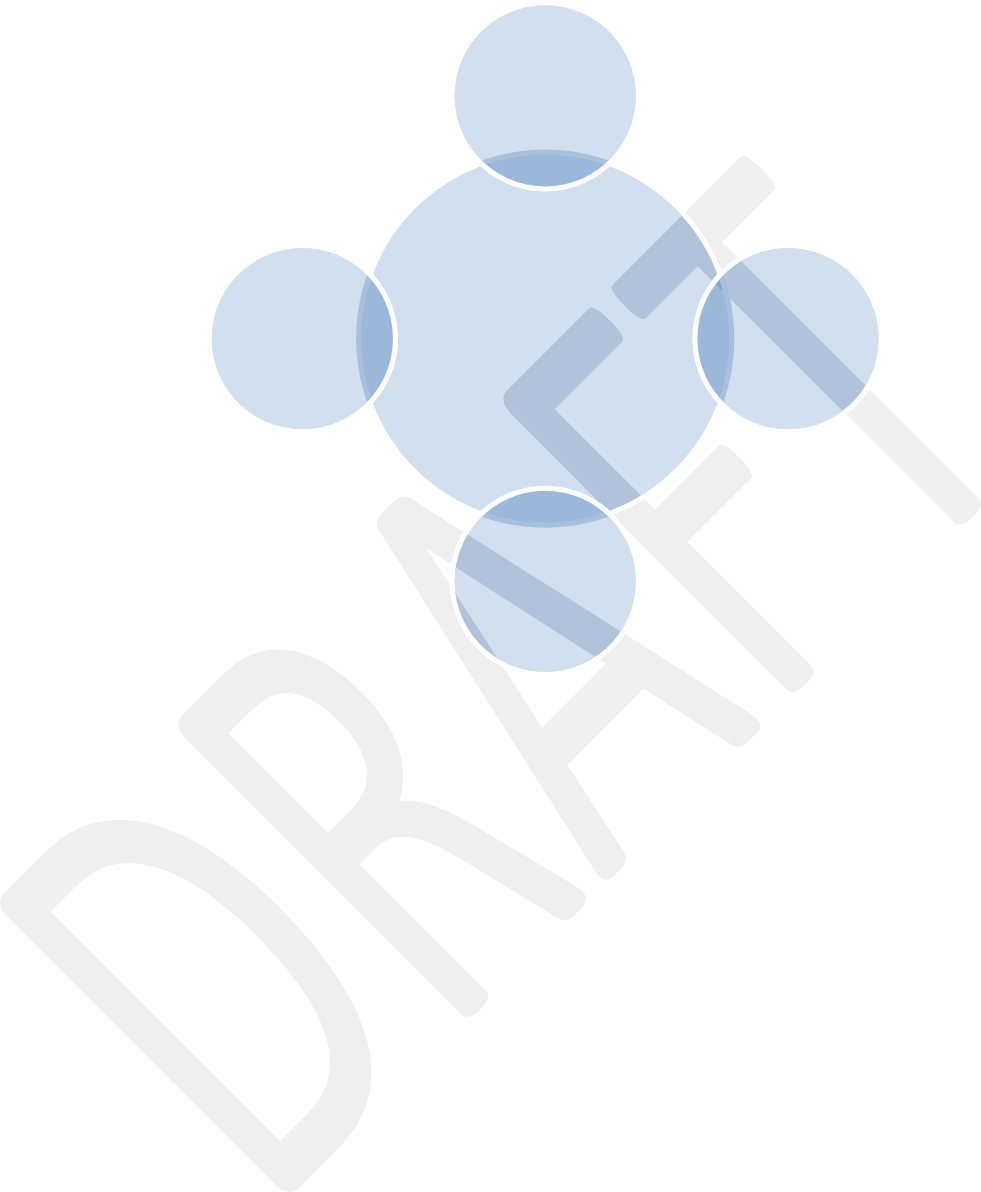
Appendix B provides the Knowledge and Skills that are required in each competency.

The list of roles provided in Appendix C can be used by course developer/IDS. Appendix C provides a more comprehensive view into the roles. This appendix expands on the functions previously identified. Specifically, Appendix C provides:

* + Function Area - which corresponds with Appendix A: Functions;
  + Role Area - these roles are guidance and may exist under different names within a particular Agency;
  + Role(s) - a general list and can be tailored to match the specific roles within the agency;
  + Responsibility of the role area;
  + Knowledge Unit - identifies the competencies associated with the role; and
  + Knowledge and Skills Table – correspondents to the knowledge unit.

#### Determination of Training Delivery

Types and methods of training need to be determined prior to the development of the training. Training methods can be self-directed, information, formal, etc. One Agency may choose to use CBT while another may use classroom presentations, seminars or some other type of formal training.

Formal

Self- directed

Training

Other

Informal

Figure 5-1 Training Methods Diagram

## Understanding the Role-Based Training Methodology

#### Purpose of Appendices

Overall, Appendices A through D provide the essential elements for developing role based training. They provide guidance and information to determine functions, outline role skills and knowledge, identifies knowledge units, and provides a method for evaluating training. Appendices E and F provide a glossary of terms and acronyms used in this document, respectively.

For the purpose of this document, Appendix A and Appendix B use the following terms:

* Competency - the quality of being adequately or well qualified in a particular area; and
* Knowledge Unit – the combination of information needed to perform a function or activity effectively and efficiently.

#### Appendix A: Functions

Appendix A is designed to assist in determining which functions and roles should be identified as candidates for role-based training. This appendix should be used by the management and training managers as well as the training developers. Additionally, the outcomes for these functions are outlined.

The format for this Appendix is as follows:

* + - * + **Function Area:** Identifies a security function area;
        + **Roles Areas:** Identifies various roles that are covered by the function. These roles are guidelines and may exist under different names within a particular Federal Organization;
        + **Definition:** Provides a definition of the function; and
        + **Learning Objectives(s):** Identifies the various outcomes that the training module should strive to meet for each of the functions and their associated roles.

#### Appendix B: Knowledge and Skill Catalog

This appendix contains each knowledge unit. Within each knowledge unit are the associated knowledge and skills. The knowledge and skills are specific and the training developer should ensure that these are covered in their training modules. This appendix should be used by the IDS/training developer, training manager, and management levels.

#### Appendix C: Roles

Appendix C is designed to assist in determining which competency/knowledge unit and associated Knowledge and Skills required by a particular role. The generic roles and job titles used within this Appendix may or may not be the same as the roles or job titles used by and individual Federal Organization. The ones used within this Appendix are a sample of current jobs/roles within various Federal Organizations and organizations at the time of publication. Using the competencies and functions, each of these samples can be tailored to meet the roles within a specific Federal Organization.

All roles should have training on the Overall Knowledge and Skills as described within Appendix B, Knowledge and Skills Catalog. These are the fundamental basis of knowledge/skills required for all jobs and roles. The IDS/training developer and training managers would be the individuals that would use this appendix.

The format is as follows:

* + - * + **Function Area**: This area corresponds with *Appendix A: Function Area*. Appendix A provides a general description of the area and the Learning Objectives for those functions. The roles described within this appendix are within a function;
        + **Role Area**: This describes the overall role;
        + **Roles**: Identifies various roles that are covered by the function. These roles are guidelines and may exist under different names within a particular Agency. Provided to assist in determining who should receive this role-based training;
        + **Responsibility**: Defines the activities, tasks and/or responsibilities of that particular role;
        + **Knowledge Unit**: Identifies the competencies associated with the role. The entire listing of the knowledge units and their associated knowledge and skills are located in *Appendix B: Knowledge and Skills Catalog*; and
        + **Corresponding Knowledge and Skills Table**: This table provides a breakdown of the specific knowledge unit, the corresponding knowledge and skills to each competency. Knowledge areas may also be referred to as “functional perspectives.” Each role has various knowledge units associated with it. There are four (4) differing functional perspectives that correspond with the job to allow for further tailoring of role-based training to better match with the job function. These functional perspectives are defined as follows:

**Manage** – those knowledge and skills particular to those employees who are responsible for management (e.g., managers, team leads, project managers)

**Design** – those knowledge and skills particular to those employees who are responsible for design activities (e.g., system developers, engineers)

**Implement** – those knowledge and skills particular to those employees who execute implementation (e.g., system administrators, network administrators)

**Evaluate** – those knowledge and skills particular to evaluation activities (e.g., testers, security analysts)

Flexibility is required for most role-based training. Tailoring is needed to allow use of the knowledge areas in accordance with respective Agency or organizational requirements. Each Agency should determine the most appropriate use of these terms.

#### Appendix D: Sample Evaluation Forms

The forms that will assist in the evaluation of the training are located within this appendix. The IDS/Training developer and training manager should use these forms.

Although this document includes a number of role-based matrices in the Appendices, this by no means suggests that any organization should have to build training courses or modules for each role. The Appendices should be viewed as a catalog of role-specific matrices, some of which will be used to build courses or modules. Organizations should have identified those personnel or roles needing role-based training, based on their having significant IT/cybersecurity responsibilities, before using NIST SP 800- 16, “*Role-Based Model for Federal Information Technology/Cybersecurity Training”*.

# Chapter 6 – Worked Example

This chapter provides two worked examples of how to use this methodology. First is the layout of the steps, which is followed by examples.

* + - * + The first step in developing role-based training is conducting the Agency-wide Needs Assessment. This action will identify any gaps in the current training program, and/or identify those roles which require training. The guidance for conducting a Needs Assessment is outside the scope of this document, but can be found in NIST SP 800-50, “*Building an Information Technology Security Awareness and Training Program”.*
        + Once this activity is completed and the role-based training area(s) identified, the second step is functions identification. Appendix A, Functions Appendix, should be seen as a catalog, whereby an organization would begin the process to develop training material for a course or module. It is important to understand that just because a function or role is listed within the appendices; it does not mean that a training course or module must be built for that role. The Needs Assessment will identify those required modules. Training must be identified, developed and provided if no such training exists for a role which the organization has identified as having significant IT/cybersecurity responsibilities. Existing training must be enhanced or a similar course identified and provided if evaluation feedback, Needs Assessment and/or job task analysis indicates that current training is not meeting the IT/cybersecurity needs of the intended audience.
        + After the functions are identified, the third step is to annotate the associated training outcomes and learning objectives. This provides the target for the training developer/IDS. Using the identified function, Appendix C will provide some associated role areas and roles and help shape the learning objectives. These provide the training developer/IDS with the ability to tailor to match the roles and terminology that the organization utilizes. Using the appropriate role, the corresponding knowledge and skills can be identified (Appendix B). Additionally, these can be further refined by the role’s functional perspective, whether that be the functional perspective of manage, design, develop or evaluate. Learning objectives should be observable and measurable and ensure they meet the organization mission.
        + In the fourth and final step the training developer can tailor the training module to the appropriate level of expertise for the audience.

Role-based training can now be developed. An example of how this would work follows.

The first activity is to conduct the Agency-wide Needs Assessment. This action will identify those role areas that require training. For this example, we will assume that the organization’s contracting office has not been including security requirements in the awarded contracts. In this example, the Needs Assessment determined that an individual has not been trained in any security areas which are identified as a training gap. The individual is a Contracts Officer, with 10 years of contracting experience and two years ago moved into IT/Cyber contracts.

The second activity is to identity the function and/or role which the training gap is associated. For this

example, the function area defined in Appendix A is Oversight, Management and Development and the role area is Procurement. The outcomes for this training are also listed in Appendix A and as the training is developed, Learning Objectives(s) should be in the forefront, (e.g., Provides contractual, procurement and/or acquisition support for purchases). Additionally, the actual job title can be traced to a Role/Function, (e.g., Procurement).

Once the function and role area has been identified, then Appendix B should be reviewed. The roles listed in Appendix C can be tailored to match those roles/job titles of the organization. At this point, the role tasks that the employee executes determine the level to which he/she needs to be trained. In our example, the Contracting Officer has 10 years of experience in contracting, but has only within the last two years moved into IT/Cybersecurity contracting. The employee is well versed and understands contracting requirements, but needs to be trained specifically on the security requirements that are associated with IT/Cyber contracting. Therefore, with only two years in IT/Cybersecurity contracting, the employee is at a Competency Level I. This competency level determines the Knowledge Units that will be used to develop the training module.

The Knowledge Unit is based on the competencies identified for that role and the knowledge and skills required to successfully execute the activities associated with the role.

In addition to the Competency levels, the functional perspective of the role must be considered. There are four (4) functional perspectives: Manage, Design, Implement and Evaluate. For this example, the role requiring training is the Contracting Officer(s) who are awarding the contracts. We will assume that the contracts have been written and this role is reviewing to ensure that the contracts are ready for award.

Therefore, we will use those knowledge and skills identified in the “Manage” column in Appendix C Module for Roles.

In the Manage column are the following competency, knowledge and skills:

* + - * + Knowledge Unit – ***Procurement***

Knowledge and Skills:

*PROC-6; PROC-7; PROC-8; PROC-9; PROC-11; PROC-12*

* + - * + Knowledge Unit – ***Management***

Knowledge and Skills:

*PM-1; PM-2; PM-3; PM-4; PM-8; PM-10; PM-12; PM-14; PM-16; PM- 22; PM-23; PM-25; PM-32; PM-33*

* + - * + Knowledge Unit – ***Compliance***

Knowledge and Skills:

*COMP-1; COMP-3; COMP-4; COMP-5; COMP-7*

Next, we will go to Appendix B. This appendix will specifically state what knowledge or skill the role contains. Using the above example, *PROC-6* means that the training module should provide the employee with knowledge about how to execute secure acquisitions.

The employee is trained specifically to his/her role as well as the corresponding responsibilities of that role. As the training module is developed, these knowledge and skills must be included with the outcome

as defined for the function.

Once the training is complete, then an evaluation should be conducted. Chapter 7 provides guidance on how to successfully evaluate the training. Appendix D provides samples forms to assist with evaluating the training. Any areas of training that were confusing or did not provide the desired outcome can be identified through the evaluation process and should be improved prior to the next training session.

This second example is to show how to do the tailoring. Using the example above, the audience receiving the training has a higher competency. The trainer may choose to concentrate the training on the skill and knowledge areas that are harder to grasp, or have been identified as weak areas by the CIO. Those skills that have been mastered may only be a small part of the training module. The purpose is to keep the audience engaged in the training.

# Chapter 7 – Training Evaluation

## Value of Evaluation in a Training Program

Evaluating training effectiveness is a vital step to ensure that the training that is delivered is meaningful. Training is meaningful *only* when it meets the needs of both the student (employee) and the organization (employer). If training content is incorrect, outdated, or inappropriate for the audience, the training will not meet student or organizational needs. If the delivery vehicle (e.g., classroom, computer-based training, and web-based training) is inappropriate, either in relation to the simplicity/complexity of the content or to the type of audience, the training will not meet the needs of the student and the organization. Spending time and resources on training that does not achieve desired effects can reinforce, rather than dispel, the perception of security as an obstacle to productivity. Further, it can require the expenditure of far more resources in data or system recovery after a security incident occurs than would have been spent in prevention activities such as training.

All meaningless training is expensive, even where the direct cost outlay, or cost-per-student, maybe low. Federal Organizations cannot afford to waste limited resources on ineffective training, consequently, evaluation of training effectiveness should become an integral component of an agency’s IT/cybersecurity training program. A robust training evaluation effort may be an effective vehicle for garnering management support for IT/cybersecurity training programs.

## Purpose of Training Evaluation

Meaningfulness of training, or its effectiveness, requires measurement. Evaluating training effectiveness has four distinct but interrelated purposes—to measure:

* The extent to which conditions were right for learning and the learner’s subjective satisfaction;
* What a given student has learned from a specific course or training event, (i.e., learning objectives and effectiveness);
* A pattern of student behavior or outcomes following a specific course or training event; (i.e., teaching effectiveness); and
* The value of the specific class or training event compared to other options in the context of an agency’s overall IT/cybersecurity training program; (i.e., program effectiveness).

An evaluation process should produce four types of measurement, each related to one of evaluation’s four purposes, as appropriate for three types of users of evaluation data:

* Evaluations should assist the employees themselves in assessing their subsequent on-the-job Performance;
* Evaluations should assist the employees’ supervisors in assessing individual students’ subsequent on-the-job performance;
* Evaluations should produce trend data to assist trainers in improving both learning and teaching; and
* Evaluations should produce Return-On-Investment (ROI) statistics to enable responsible officials to allocates limited resources in a thoughtful, strategic manner among the spectrum of

security awareness, cybersecurity essentials, role-based security training, and education options for optimal results among the workforce as a whole.

## Development of an Evaluation Plan

It is often difficult to get good information for each of the evaluation’s four purposes, as described above, and it is impossible to do so without conducting appropriate planning for an evaluation. To evaluate student learning, it is first necessary to have written learning objectives, stated in an observable, measurable way as Learning Objectives or behavioral objectives. To evaluate teaching, it is necessary to plan for the collection of trend data, evaluation, and extrapolation. To evaluate ROI mission-related goals must be explicitly identified to which the learning objectives are related. The remainder of this section provides guidance in the development of an Evaluation Plan.

#### Behavioral Objectives

The major components of behavioral objectives are:

* Conditions of Activity – written description of the existing conditions and the learning activity;
* Activity to be Performed – how the activity will be performed in order to allow the student to learn; and
* Level of Success – how has the student’s performance on the job changed as a result of the information learned.

There are several schools of behavioral objectives among educational theorists; however, most agree with the three components, described below.

#### Conditions of Activity

This is a written description of existing conditions prior to, and in preparation for, the learning activity. Certain conditions must be present to forecast training effectiveness. Does the student need a checklist, a set of items to manipulate, or an outline of the information? Does the instructor need audiovisual equipment, handouts, or a classroom with furniture set up in a specific format? Conditions of the learning activity, including CBT not just platform training, must be specific and comprehensive.

### Activity to be Performed

The evaluation plan must state the activity to be performed in a manner permitting the evaluator to actually observe the behavior that the student is to learn—which is observable in class (teacher as evaluator) or back on the job (supervisor as evaluator). It is difficult, if not impossible, to measure the process of a student’s changing attitude or thinking through a task or problem. The evaluator, however, can measure a written exercise, a skill demonstration, a verbal or written pronouncement, or any combination of these outwardly demonstrable activities. He/she cannot take the student’s word for the learned skill, or rely on the simple fact that the student was present and exposed to the skill or information being taught. Rather, the evaluator must observe the skill being performed or the information being applied. With CBT, evaluation measurement can be programmed to occur at the instructional block level, with subsequent blocks adjusted based on a student’s response. Platform training differs from CBT since platform training has an instructor in the classroom. With platform training, adjustments can be made in real time by the instructor based on the nature of student questions during the course. Adjustments can also be made between courses in a student’s training sequence.

### Levels of Success

Measures of success should be derived from the individual’s normal work products rather than from classroom testing. This directly ties the individual’s performance to its impact on the organization’s mission. Written behavioral objectives for a learning activity must include a stated level of success. For quantitative skills, must the learner perform successfully every time, or 10 out of 100 times, or 5 out of 10 times in terms of performance requirements or consequences? Risk management requirements should be used to establish the criticality of quantitative skills. For qualitative skills, what distinguishes satisfactory performance from failure, or outstanding performance from satisfactory? Measurements of qualitative skills might include the amount of re-work required, customer satisfaction, or peer recognition of the employee as a source of IT/cybersecurity information.

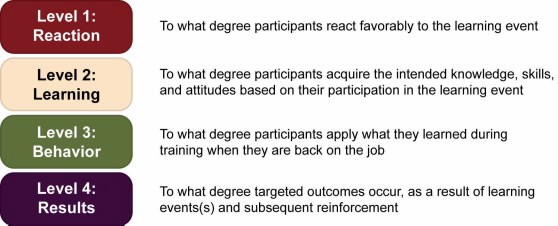
The nature and purpose of the training activity, and whether it is at a beginning, intermediate, or advanced level, will influence the setting of success measures. If success levels are not documented, an individual student’s achievement of the behavioral objectives of the learning activity can not be evaluated, nor can the learning activity itself be evaluated within an organization’s overall training program.

In addition to the written objectives suggested above, the evaluation plan should show how the collected data is to be used to support the cost and effort of the data collection. This can be related to types of evaluations, presented next.

#### Types of Evaluations

One type of evaluation is to conduct an exercise that allows training participants to test/validate the knowledge of learned behavior following courses. Through this exercise, the trainer can identify areas that may need improvement.

Another type of evaluation is the Kirkpatrick model which was introduced in 1959:



For all types of evaluation, a critical step is to ensure the feedback is considered in the continuous training process. Regardless of the type of evaluation that is implemented, the feedback must be looped back into

the training material. For example, if a student states that Chapter Two (2) was vague, that chapter should be updated for clarity prior to the next training session.

### Student Satisfaction

A common term for this type of evaluation is the ‘Smiley Face’ evaluation. Likert Scale-type forms ask the student to check a range of options from poor to excellent (or *vice versa*) to indicate how he/she felt about the class, the computer-based courseware, or whatever the learning activity was. The response data is an indicator of how the learning activity is received by the student. The responses also reveal if the conditions for learning were correct. Some of the questions in this level of evaluation ask about the student’s satisfaction with the training facility and instructor (if classroom training), the manner of presentation (of the content), and whether or not course objectives were met in relation to the student’s expectations. Although this type of evaluation does not provide in-depth data, it does provide rapid feedback from the learner’s perspective. Measurement of training effectiveness depends on an understanding of the background and skill level of the training audience.

### Learning and Teaching Effectiveness

This level of evaluation measures how much information or skill was transmitted from the training activity to the learner or student. The evaluation should be in various formats relative to the level of training. For example, at an intermediate or advanced role-based training level, participants should be given some sort of performance test, such as a case study to solve. The evaluation format must relate back to the behavioral objectives of the learning activity, which, in turn, drives the content being presented. The evaluation also provides instant feedback, and it assesses how much the student remembered or demonstrated by skill performance by the end of the program, not how he/she felt about it. Evaluation can be built into each block of instruction and does not need to wait until the end of a course.

An evaluation measures success in transference of information and skills to the student. It enables the evaluator to determine if a given student may need to repeat the course, or perhaps attend a different type of learning activity presenting the same material in a different format (if available). The evaluator should be able to see if a pattern of transference problems emerges, and determine whether or not the course itself may need to be reconfigured or perhaps dropped from an organization’s training program.

Behavior objective testing is possibly the most difficult measurement area to address. It is relatively easy to test the knowledge level of the attendees after completing a course or block of instruction, but it is not easy to determine when that learning took place. An attendee may have had knowledge of the subject area before receiving the instruction, so the course may have had little or no impact. Thus, information collected solely at the conclusion of a course/instructional block must be examined relative to the attendee’s background and education.

To better determine the learning impact of a specific course or instructional block, one approach is to use pre/post-testing, in which a test or testing is performed at the outset of the course. The results are then compared to testing conducted at the conclusion of instruction.

Testing of an attendee’s knowledge of a particular subject area by including questions or tasks where there is a single right answer or approach, is appropriate for almost all testing situations, especially at the beginning and intermediate levels. Questions regarding selection of the best answer among possible options should be reserved for those training environments where there is opportunity for analysis regarding why a particular answer is better than other answers.

### Student Performance Effectiveness

This evaluation is the first level which asks for more than student input. At this level, the evaluator, through a structured questionnaire usually administered 30 to 60 days following the training activity, asks the supervisor about the performance of the employee(s) relative to the behavioral objectives of the course. This is a before and after job skills comparison. In some cases this information is difficult to obtain, especially when employees’ roles and seniority levels permit them considerable autonomy, without direct supervision. When supervisors observe only the final output of employee actions, developing a valid questionnaire can present a particular challenge. When accomplished successfully, a Level 3 evaluation should begin to show the extent to which the learning activity benefits the organization as well as the employee. The learner’s supervisor may determine whether the learner used the knowledge obtained in the course to accomplish job tasks, or whether the learner’s performance improved since taking the course.

### Assessing Training Program Effectiveness

This assessment is done by collecting data on whether the participants were satisfied with the deliverables of the training program, whether they learned something from the training and if they are able to apply those skills at their workplace

Evaluations can be difficult to undertake and hard to quantify. They can involve structured, follow-up interviews with students, their supervisors, and colleagues. They can involve comparison of outputs produced by a student both before and after training by a subject-matter expert. They can involve some form of benchmarking or evaluation of the particular training activity in relation to other options for a particular job performance measure. In all cases, they involve quantifying the value of resulting improvement in relation to the cost of training. Evaluations, properly designed, can help senior management officials to answer such hypothetical questions as: “Is it more cost-effective to devote limited training resources to the education of a single, newly-appointed IT/cybersecurity specialist in this organization, or to devote the same resources to Cybersecurity Essentials training of all employees in the organization?”; or “Is it a better return on investment to train ‘front-end’ systems designers and developers in building security rules commensurate with the sensitivity of the system, or to train ‘back- end’ users in compliance with currently existing system rules?”

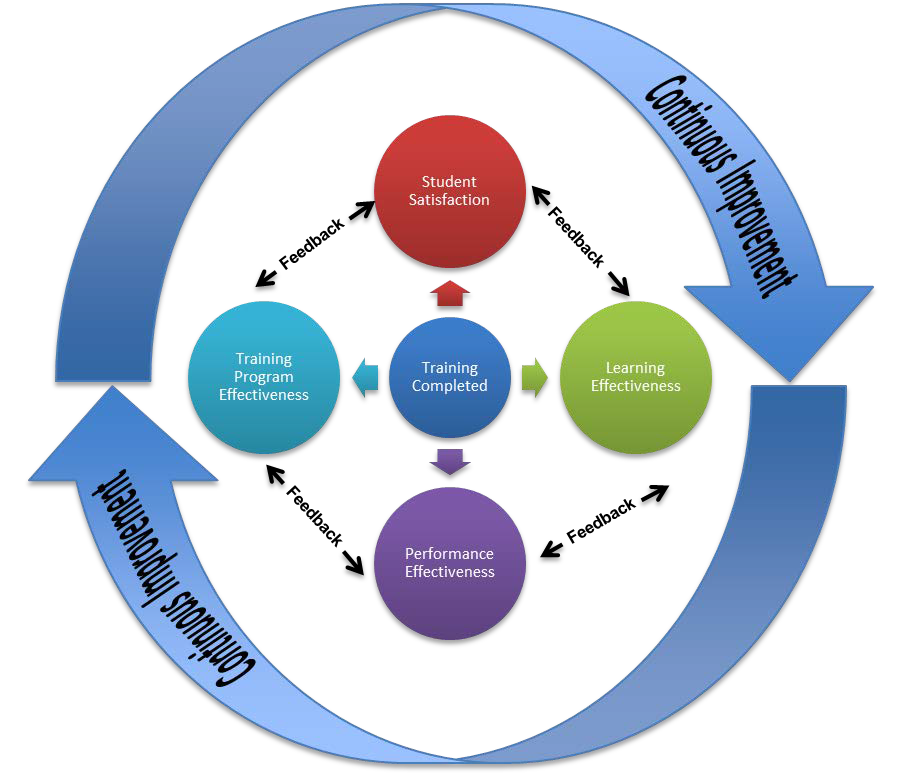


Figure 7-1 Continuous Improvement

## Importance of Feedback

Critical to the evaluation process is that the feedback obtained be looped back into the training material. Thus, there is a continuous process of training, evaluation and then updating the training prior to the next presentation.

There are benefits that come with a good evaluation plan. First, evaluation ensures accountability which means that the evaluation ensures that training programs address the training gaps. Second, it assesses the cost and monies spent: evaluation ensures that the training programs are effective in improving the work quality, employee behavior, attitude and develop new skills and enhance old skills within a budget.

Lastly, and, maybe most importantly, evaluations provide feedback to the trainer on the entire training process. Since evaluations access individuals at their work level, it is easier to understand and recognize the training loopholes and incorporate required changes in the training methodology.

# Appendix A: Functions

This Appendix is designed to assist in determining which functions and roles should be identified as candidates for role-based training. Additionally, the outcomes for these functions are outlined.

Please note that the roles and Learning Objectives are guidelines, and can be tailored to meet the specific needs of an Agency or organization.

Functions associated with specific areas, such as “Collection and Targets”, are not covered within this document. These exist but are considered highly specialized areas. For these functions, the identification of roles and outcomes can be selected by the Agency.

The format for this Appendix is as follows:

* **Function Area:** Identifies a security function area;
* **Roles Areas:** Identifies various roles that are covered by the function. These roles are guidelines and may exist under different names within a particular Agency;
* **Definition:** Provides a definition of the function; and
* **Outcome(s):** Identifies the various outcomes that the training module should strive to meet for each of the functions and their associated roles.

INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Functions Function Area: **Oversight, Management and Support**

Role Areas:

* + Legal Advice and Advocacy
  + Strategic Planning and Policy Development
  + Awareness, Education and Training
  + Privacy
  + Management
  + Procurement
  + Personnel Security
  + Physical and Environmental Security
  + Security Program Management

**Definition** — Provides oversight and support so that others may effectively conduct Cybersecurity work.

**Learning Objectives** —An individual should be able to successfully complete one or all of the following, depending on the role(s):

* + Provide legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain.
  + Advocate legal and policy changes and make a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
  + Apply knowledge of priorities to define an entity’s direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest.
  + Develop policy or advocate for changes in policy that will support new initiatives or required change/enhancements.
  + Conduct training of personnel within pertinent subject domains.
  + Develop, plan, coordinate and evaluate training courses, methods, and techniques as appropriate.
  + Oversees the security baseline and associated activities of an information system in or outside the network environment.
  + Provides contractual, procurement and/or acquisition support for IA purchases.
  + Manage IT/cybersecurity implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement emergency planning, security awareness, and other resources.
  + Ensures that privacy impact assessments are conducted and appropriate controls are implemented.
  + Ensures physical controls are correctly implemented.
  + Provides personnel security policies, implements security controls and handles all personnel issues.

INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Functions

Function Area: **Securely Provision/Develop**

Role Areas:

* + Compliance
  + Software Assurance and Software Engineering
  + Systems Security and Enterprise Architecture
  + Technology Research and Development
  + Systems Requirements Planning
  + Test and Evaluation
  + Systems Development

**Definition** — Addresses areas concerned with conceptualizing, designing, and building Information Technology systems, with the responsibility for some aspect of the systems’ development.

**Learning Objectives** —An individual should be able to successfully complete one or all of the following, depending on the role(s):

* + Oversee, evaluate and support the documentation, validation, and accreditation processes.
  + Validate security compliance from internal and external perspectives.
  + Develop, create, and write/code new (or modify existing) computer applications, software, or specialized utility programs.
  + Develop system concepts and work on the capabilities phases of the systems development lifecycle.
  + Translate technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
  + Conduct technology assessment and integration processes.
  + Provide and support a prototype capability and evaluate its utility.
  + Consult with customers to gather and evaluate functional requirements and translate these requirements into technical solutions.
  + Provide guidance to customers about applicability of information systems to meet business needs.
  + Develop and conduct tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics, including interoperability, of systems or elements of system incorporating information technology.
  + Work on the development phases of the systems development lifecycle.

INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Curriculum Module for Functions

Function Area: **Operate and Maintain**

Role Areas:

* + Data Administration
  + Knowledge Management
  + Information Systems Security Operations
  + Customer Service and Technical Support
  + Network Services
  + System Administration
  + System Security Analysis

**Definition** — Responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient information technology system performance and security.

**Learning Objectives** —An individual should be able to successfully complete one or all of the following, depending on the role(s):

* + Develop and administer databases and/or data management systems that allow for the storage, query, and utilization of data.
  + Oversee the information assurance program of an information system inside or outside the network environment.
  + Manage and administer processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
  + Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries.
  + Install, configure, test, operate, maintain, and manage the networks and their firewalls, including hardware and software, that permit the sharing and transmissions of information to support the security of the information and information systems.
  + Install, configure, troubleshoot, and maintain server configurations to ensure their confidentiality, integrity, and availability.
  + Manage accounts, firewalls, and patches.
  + Create and administer access control, passwords and accounts.
  + Conduct the integration/testing, operations and maintenance of system security.

INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Functions

Function Area: **Assess/Evaluate**

Role Areas:

* + Computer Network Defense Analysis
  + Incident Response and Handling
  + Computer Network Defense Infrastructure Support
  + Vulnerability Assessment and Management
  + Risk Analysis and Management

**Definition** —Responsible for the identification, analysis and mitigation of vulnerabilities and threats to information technology system or networks.

**Learning Objectives** —An individual should be able to successfully complete one or all of the following, depending on the role(s):

* + Ability to use defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems and networks from threats.
  + Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.
  + Develop and/or recommend appropriate mitigation countermeasures in operational and non- operational situations.
  + Test, implement, deploy maintain and administer the infrastructure hardware and software that are required to effectively manage the computer network defense service to provider network and resources.
  + Manage relevant security implications within the organization, specific program, or other area of responsibility. This includes strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.
  + Conduct assessment of threats and vulnerabilities.
  + Determine deviations from acceptable configurations, enterprise or local policy.
  + Assess the level of risk.

INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Functions

Function Area: **Respond/Investigate**

Role Areas:

* + Investigation
  + Digital Forensics

**Definition** — Responsible for the investigation of cyber events and/or crimes of IT systems, networks, and safeguarding digital evidence.

**Learning Objectives** —An individual should be able to successfully complete one of all of the following, depending on the role(s):

* + Apply tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection.
  + Appropriately balance the benefits of prosecution versus intelligence gathering.
  + Collect, process, preserve, analyze and present computer-related evidence in support of network vulnerability mitigation, and/or criminal fraud, counterintelligence or law enforcement investigations.
  + Investigate and analyze all relevant response activities.

INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Functions

Function Area: **Continuous Monitoring**

Role Areas:

* + System Administration
  + Vulnerability Assessment
  + Trend Analysis
  + Risk Management
  + Maintain/upgrade industry standard encryption algorithms, key sizes; and on-going renewal/upgrade of digital certificates.

**Definition** — Promotes near real-time risk management and ongoing system authorization.

**Learning Objectives** —An individual should be able to successfully complete one of all of the following, depending on the role(s):

* + Monitor network to actively remediate unauthorized activities.
  + Identify trends.
  + Understand vulnerabilities and identify false negatives.

INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Functions

Function Area: **Contingency Planning**

Role Areas:

* + IT Disaster Recovery
  + Enterprise Continuity
  + Business Impact Analysis
  + Training and Exercises
  + First Response

**Definition** — Plan and prepare for response to an unplanned event, specific system failure, or disruption of operations.

**Learning Objectives** —An individual should be able to successfully complete one of all of the following, depending on the role(s):

* + Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, and preservation of property.
  + Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of information and maintain IT/cybersecurity.
  + Analyses business functions and IT requirements to determine impact to the organization and identify critical systems and applications.
  + Conduct training and exercises of implemented plans and procedures to determine effectiveness.

# Appendix B: Knowledge and Skills Catalog

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
|  |  |
|  | **Overall** |
| OV-1 | Skill in communicating both orally and in writing |
| OV-2 | Knowledge of fundamental Information Awareness concepts |
| OV-3 | Knowledge of the Risk Management Framework and corresponding guidance |
| OV-4 | Knowledge of the NIST SP 800-53, “*Guide for Assessing the Security Controls in Federal Information*  *Systems”* security controls and corresponding guidance |
| OV-5 | Knowledge of technical documents and reports |
| OV-6 | Skill in problem solving |
| OV-7 | Knowledge of quality assurance |
| OV-8 | Skill in reasoning techniques |
| OV-9 | Knowledge of organizational awareness |
| OV-10 | Knowledge of risks introduced by social media |
| OV-11 | Knowledge of ethical standards |
| OV-12 | Skill in ethical testing and implementation of security controls |
| OV-13 | Knowledge of mathematical reasoning |
|  | **Advanced Network Technology and Protocols** |
| ANTP-1 | Knowledge of mobile technologies |
| ANTP-2 | Skill in implementing and securing mobile technologies |
| ANTP-3 | Skill in implementing advanced protocols |
| ANTP-4 | Knowledge of security impacts of advanced network technology and protocols |
| ANTP-5 | Knowledge of how advanced network services and protocols interact to provide network communications |
|  | **Architecture** |
| ARCH-1 | Knowledge of embedded systems |
| ARCH-2 | Knowledge of digital rights management |
| ARCH-3 | Knowledge of VPN security |
| ARCH-4 | Skill in using VPN devices and encryption |
| ARCH-5 | Knowledge of IT architecture concepts and frameworks |
| ARCH-6 | Knowledge of parallel and distributed computing concepts |
| ARCH-7 | Knowledge of remote access technology concepts |
| ARCH-8 | Knowledge of the enterprise IT architecture |
| ARCH-9 | Knowledge of communication methods, principles, and concepts that support the network infrastructure |
| ARCH-10 | Knowledge of computer networking fundamentals |
| ARCH-11 | Knowledge of the common networking protocols, services, and how they interact to provide network  communications |
| ARCH-12 | Knowledge of routing principles |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| ARCH-13 | Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not used  standard IT) for safety, performance, and reliability |
| ARCH-14 | Knowledge of enterprise messaging systems and associated software |
| ARCH-15 | Knowledge of the organization’s enterprise IT goals and objectives |
| ARCH-16 | Skill in implementing the methods, standards, and approaches for describing, analyzing, and documenting  an organization's enterprise IT architecture |
| ARCH-17 | Skill in analyzing and securing an enterprise architecture |
| ARCH-18 | Knowledge of industry-standard and organizationally accepted security principles and methods |
| ARCH-19 | Knowledge of engineering concepts |
| ARCH-20 | Knowledge of structured analysis principles and methods |
| ARCH-21 | Knowledge of system design tools, methods, and techniques, including automated systems analysis and  design tools |
|  | **COMPLIANCE** |
| COMP-1 | Skill in tracking and analyzing technical and legal trends that will impact cyber activities |
| COMP-2 | Skill in determining impact of technology trend data on laws, regulations, and/or policies |
| COMP-3 | Knowledge of International Traffic in Arms Regulations and relevance to cybersecurity |
| COMP-4 | Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, HIPAA, PCI-DSS, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Executive Orders, Presidential  Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed |
| COMP-5 | Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact  critical infrastructure |
| COMP-6 | Skill in identifying the risks associated with social media |
| COMP-7 | Knowledge of Personally Identifying Information (PII) and personal Payment Card Industry (PCI) data  security standards |
| COMP-8 | Skill in developing and executing test methodologies to ensure compliance to directives (Policy and/or  technical) |
| COMP-9 | Knowledge of rationale for organizationally defined auditable events |
| COMP-10 | Knowledge of technical and legal trends that impact cyber activities |
|  | **COMPUTER NETWORK DEFENSE** |
| CND–1 | Knowledge of Computer Network Defense and vulnerability assessment tools, including open source tools,  and their capabilities |
| CND–2 | Knowledge of intrusion detection and prevention system tools and applications |
| CND–3 | Knowledge of Content dev |
| CND–4 | Knowledge of the types of intrusion detection and prevention system hardware and software |
| CND–5 | Skill in handling malware |
| CND-6 | Skill in detecting host and network-based intrusions via intrusion detection and prevention, and other  network monitoring tools |
| CND– 7 | Skill in mimicking threat behaviors |
| CND–8 | Skill in tuning security monitoring sensors |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| CND–9 | Knowledge of Insider Threat investigations, reporting, investigative tools, and laws/regulations |
| CND–10 | Knowledge of computer network operations methodologies, including analysis and exploitation |
| CND–11 | Knowledge of common adversary capabilities, tactics, techniques, and procedures in assigned area of  responsibility |
| CND–12 | Knowledge of Defense-In-Depth principles and network security architecture |
| CND–13 | Skill in collecting data from a variety of Computer Network Defense resources |
| CND-4 | Skill in protecting a network against malware |
| CND–15 | Knowledge of Computer Network Defense policies, procedures, and regulations |
| CND – 16 | Knowledge of the common attack vectors on the network layer |
| CND – 17 | Knowledge of different classes of attacks |
| CND – 18 | Knowledge of operational threat environments |
| CND – 19 | Knowledge of malware analysis concepts and methodology |
| CND – 20 | Knowledge of general attack stages |
| CND – 21 | Skill in deep analysis of captured malicious code |
| CND – 22 | Knowledge of malware analysis and tools |
| CND – 23 | Knowledge of virtual machine aware malware, debugger aware malware, and packing |
| CND -24 | Skill in analyzing anomalous code as malicious or benign |
| CND – 25 | Skill in identifying obfuscation techniques and removing the malware |
| CND-26 | Skill in conducting investigations and developing comprehensive reports |
| CND – 27 | Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures |
| CND-28 | Skill in malware analysis |
| CND-29 | Knowledge of the CND Service Provider reporting structure and processes within one’s own organization |
| CND-30 | Skill in de-conflicting cyber operations and activities from operational activities |
|  | **CONFIGURATION MANAGEMENT** |
| CM – 1 | Knowledge of secure configuration management techniques |
| CM-2 | Skill in developing configuration baselines per appropriate hardening guides |
| CM-3 | Skill in documenting configuration settings |
| CM-4 | Skill in security impact analysis of changes to the configuration |
| CM-5 | Knowledge of configuration change control |
| CM-6 | Knowledge of access restrictions for change |
| CM-7 | Skill in developing configuration management policy and procedures |
| CM-8 | Skill in maintaining configuration baseline of the information system |
| CM-9 | Knowledge of information system component inventory |
| CM-10 | Skill in developing information system component inventory |
| CM-11 | Knowledge of configuration management plan and how it is used |
| CM-12 | Skill in developing configuration management plan |
| CM-13 | Knowledge of configuration management requirements for developers |
| CM-14 | Skill in implementing configuration change controls |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| CM-15 | Skill in implementing configuration management plan |
|  | **CRYPTOGRAPHY AND ENCRYPTION** |
| CR -1 | Knowledge of encryption methodologies |
| CR – 2 | Knowledge of encryption algorithms |
| CR -3 | Knowledge of cryptography |
| CR-4 | Knowledge of cryptographic implementation |
| CR-5 | Knowledge of certificate management infrastructures |
| CR-6 | Skill in encryption methodologies |
| CR-7 | Skill in cryptography implementation |
| CR-8 | Skill in decryption if digital data |
| CR-9 | Skill in one way hash functions |
| CR-10 | Knowledge of computer algorithms |
| CR-11 | Skills in implementing the FIPS validated cryptography |
| CR-12 | Skill in implementing and maintaining transmission confidentiality and integrity |
| CR-13 | Skill in implementing NSA approved cryptography |
| CR-14 | Knowledge of FIPS validated cryptography |
| CR-15 | Knowledge of NSA approved cryptography |
|  | **DATA SECURITY** |
| DS-1 | Skill in analyzing network traffic capacity and performance characteristics |
| DS-2 | Knowledge of data administration and data standardization policies and standards |
| DS-3 | Knowledge of data mining and data warehousing principles |
| DS-4 | Knowledge of sources, characteristics, and uses of the organization’s data assets |
| DS-5 | Knowledge of the capabilities and functionality associated with various technologies for organizing and  managing information |
| DS-6 | Knowledge of the characteristics of physical and virtual data storage media |
| DS-7 | Skill in developing data dictionaries |
| DS-8 | Skill in developing data repositories |
| DS-9 | Skill in data mining techniques |
| DS-10 | Knowledge of database theory |
| DS-11 | Skill in data reduction |
| DS-12 | Skill in the interpretation and incorporation of data from multiple tool sources |
| DS-13 | Knowledge of complex data structures |
| DS-14 | Knowledge of computer programming principles such as object-oriented design |
| DS-15 | Skill in Data Loss Prevention technologies (DLP) |
| DS-16 | Knowledge of logical access to system functions |
| DS-17 | Skill in enforcing logical access controls |
| DS-18 | Skill in enforcement of information flow policies |
|  | **DATABASE** |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| DB-1 | Skill in allocating storage capacity in the design of database management systems |
| DB-2 | Skill in designing databases |
| DB-3 | Skill in optimizing database performance |
| DB-4 | Knowledge of database management systems, query languages, table relationships, and views |
| DB-5 | Knowledge of database systems |
| DB-6 | Knowledge of query languages |
| DB-7 | Skill in conducting queries and developing algorithms to analyze data structures |
| DB-8 | Skill in generating queries and reports |
| DB-9 | Skill in maintaining databases |
| DB-10 | Skill in implementing backup plans |
| DB-11 | Skill in implementing maintenance plans |
|  | **DIGITAL FORENSICS** |
| DF-1 | Knowledge of seizing and preserving digital evidence |
| DF-2 | Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration,  loss, physical damage, or destruction of data |
| DF-3 | Skill in setting up a forensic workstation |
| DF-4 | Knowledge of basic concepts and practices of processing digital forensic data |
| DF-5 | Skill in analyzing memory dumps to extract information |
| DF-6 | Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools |
| DF-7 | Knowledge of server diagnostic tools and fault identification techniques |
| DF-8 | Skill in preserving evidence integrity according to standard operating procedures or national standards |
| DF-9 | Knowledge of investigative implications of hardware, Operating Systems, and network technologies |
| DF-10 | Knowledge of types and collection of persistent data |
| DF-11 | Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant  information and where to find those system files |
| DF-12 | Skill in identifying and extracting data of forensic interest in diverse media |
| DF-13 | Skill in using forensic tool suites |
| DF-14 | Knowledge of types of digital forensics data and how to recognize them |
| DF-15 | Knowledge of deployable forensic software to perform forensic imaging remotely |
| DF-16 | Skill in conducting forensic analyses in multiple operating system environments |
| DF-17 | Skill in decrypting digital data collections |
| DF-18 | Skill in identifying forensic footprints |
| DF-19 | Knowledge of data carving tools and techniques |
| DF-20 | Knowledge of anti-forensics tactics, techniques, and procedures |
| DF-21 | Knowledge of common forensics tool configuration and support applications |
| DF-22 | Skill in analyzing volatile data |
| DF-23 | Knowledge of legal governance related to admissibility, such as Federal Rules of Evidence |
| DF-24 | Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid  alteration, loss, physical damage, or destruction of data |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| DF-25 | Knowledge of electronic evidence law |
| DF-26 | Knowledge of legal rules of evidence and court procedure |
| DF-27 | Knowledge of file system geometry in multiple operating systems |
| DF-28 | Knowledge of mobile device forensics |
| DF-29 | Knowledge of image acquisition and validation |
| DF-30 | Skill in retrieving forensic information from information system backups |
| DF-31 | Skill in recognizing security incident trends in forensic data |
|  | **EMERGING TECHNOLOGIES** |
| ET-1 | Knowledge of new and emerging IT and IT/cybersecurity technologies |
| ET-2 | Knowledge of new technological developments in server administration |
| ET-3 | Knowledge of the capabilities and functionality associated with various content creation technologies |
| ET-4 | Knowledge of the capabilities and functionality of various collaborative technologies |
| ET-5 | Skill in applying and incorporating IT technologies into proposed solutions |
| ET-6 | Skill in the determination of the validity of technology trend data |
| ET-7 | Knowledge of emerging computer-based technology that have potential for exploitation by adversaries |
| ET-8 | Knowledge of industry indicators useful for identifying technology trends |
| ET-9 | Knowledge of products and nomenclature of major vendors and how differences affect  exploitation/vulnerabilities |
| ET-10 | Knowledge of emerging security issues, risks, and vulnerabilities |
| ET-11 | Knowledge of cloud computing environments and the risks |
|  | **ENTERPRISE CONTINUITY** |
| ECP-1 | Knowledge of disaster recovery and continuity of operations plans |
| ECP-2 | Knowledge of enterprise continuity response program, roles, and responsibilities |
| ECP-3 | Skill in developing disaster recovery and continuity of operations plans |
| ECP-4 | Skill in executing disaster recovery and continuity of operations plans |
| ECP-5 | Knowledge of enterprise continuity planning |
| ECP-6 | Skill in conducting Business Impact Assessments |
| ECP-7 | Skill in developing disaster recovery and continuity of operations strategies |
| ECP-8 | Skill in developing enterprise business continuity plans |
| ECP-9 | Skill in exercising and maintaining enterprise business continuity plans |
| ECP-10 | Skill in developing, testing, and implementing network infrastructure contingency and recovery plans |
| ECP-11 | Skill in performing damage assessments |
| ECP-12 | Skill in testing use of alternate storage site |
| ECP-13 | Skill in testing use of alternate processing site |
| ECP-14 | Knowledge of alternate telecommunication services for primary and alternate processing or storage sites |
| ECP-15 | Knowledge of location of information system backups and their recovery procedures |
| ECP-16 | Knowledge of activities involved in information system recovery and reconstitution |
| ECP-17 | Skill in performing activities involved in information system recovery and reconstitution |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| ECP-18 | Skill in assessing and employing organization defined security controls at alternate work sites |
|  | **IDENTITY MANAGEMENT/PRIVACY** |
| IM-1 | Knowledge of access authentication methods |
| IM-2 | Knowledge of network access, identity and access management |
| IM-3 | Knowledge of policy-based and risk adaptive access controls |
| IM-4 | Skill in applying host/network access controls |
| IM-5 | Skill in developing and applying security system access controls |
| IM-6 | Skill in maintaining directory services |
| IM-7 | Knowledge of organizational IT user security policies |
| IM-8 | Skill in identifying privacy issues and associated mitigation |
| IM-9 | Knowledge of collection, use, maintenance and sharing of PII |
| IM-10 | Skill in conducting Privacy Impact Assessment |
| IM-11 | Skill in monitoring and auditing privacy controls and internal privacy policies |
|  | **INCIDENT MANAGEMENT** |
| IR-1 | Knowledge of procedures used for documenting and querying reported incidents |
| IR-2 | Knowledge of incident categories, incident responses, and timelines for responses |
| IR-3 | Knowledge of incident response and handling methodologies |
| IR-4 | Skill in recovering failed servers |
| IR-5 | Skill in using incident handling methodologies |
| IR-6 | Knowledge of enterprise incident response program, roles, and responsibilities |
| IR-7 | Knowledge of root cause analysis for incidents |
| IR-8 | Skill in performing root cause analysis for incidents |
| IR-9 | Skill in isolating compromised systems |
| IR-10 | Knowledge in performing traffic analysis |
| IR-11 | Knowledge of secure transfer of evidence to forensics |
| IR-12 | Skill in security monitoring to determine possible incidents |
| IR-13 | Skill to correlate and combine data to develop information about the capabilities, intent, and operations of  criminal and/or adversary organizations |
| IR-14 | Skill in recognizing and categorizing types of vulnerabilities and associated attacks |
| IR-15 | Skill in performing damage assessments from incidents |
| IR-16 | Knowledge of processes for reporting security related incidents |
| IR-17 | Skill in monitoring and evaluating security incident trends |
| IR-18 | Knowledge that security incident trends exist |
| IR-19 | Skill in providing incident response support |
| IR-20 | Knowledge of security alerts, advisories, and directives |
|  | **INDUSTRIAL CONTROL SYSTEMS** |
| ICS-1 | Knowledge of risk(s) specific to Industrial Control Systems (ICS) |
| ICS-2 | Knowledge of ICS unique performance and reliability requirements |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| ICS-3 | Skill in restricting logical access to the ICS network and network activity |
| ICS-4 | Skill in restricting physical access to the ICS network and devices |
| ICS-5 | Skill in protecting individual ICS components from exploitation |
| ICS-6 | Skill in maintaining functionality during adverse conditions |
| ICS-7 | Skill in restoring ICS after incident quickly |
|  | **INFORMATION ASSURANCE** |
| IA-1 | Knowledge of Security Assessment and Authorization process |
| IA-2 | Knowledge of IA principles used to manage risks related to the use, processing, storage, and transmission  of information or data |
| IA-3 | Knowledge of IA principles and methods that apply to software development |
| IA-4 | Knowledge of IA principles and organizational requirements (relevant to confidentiality, integrity,  availability, authentication, non-repudiation) |
| IA-5 | Knowledge of security management |
| IA-6 | Skill in designing security controls based on IA principles and tenets |
| IA-7 | Skill in determining how an information system should work (including its resilience and dependability  capabilities) and how changes in conditions, operations, or the environment will affect these outcomes |
| IA-8 | Skill in securing network communications |
| IA-9 | Knowledge of various means to validate information system input |
|  | **WEB SECURITY** |
| WT-1 | Knowledge of web services |
| WT-2 | Knowledge of web collection, session management, searching/analyzing techniques, tools, and cookies |
| WT-3 | Knowledge of web filtering technologies |
| WT-4 | Knowledge of OWASP, ISO, and other standards relating to web based applications |
| WT-5 | Skill in building, designing and testing the security of web applications and web services |
| WT-6 | Knowledge of common web application attack vectors |
| WT-7 | Knowledge of user input validation techniques for web applications |
| WT-8 | Skill in performing web applications testing |
| WT-9 | Knowledge of web applications firewalls |
| WT-10 | Skill in training authorized individuals to ensure that publicly accessible information does not contain  nonpublic information |
|  | **INFORMATION SYSTEMS** |
| SI-1 | Knowledge of how system components are installed, integrated, and optimized |
| SI-2 | Knowledge of principles and methods for integrating server components |
| SI-3 | Knowledge of technology integration processes |
| SI-4 | Skill in designing the integration of hardware and software solutions |
| SI-5 | Knowledge of operating systems |
| SI-6 | Knowledge of server and client operating systems |
| SI-7 | Knowledge of systems administration concepts |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| SI-8 | Skill in system administration for operating systems |
| SI-9 | Knowledge of file system implementations |
| SI-10 | Knowledge of virtualization technologies and virtual machine development and maintenance |
| SI-11 | Knowledge of command lines |
| SI-12 | Skill in identifying, modifying, and manipulating applicable system components |
| SI-13 | Skill in reading, interpreting, writing, modifying, and executing simple scripts on systems that perform  tasks like parsing large data files, automating manual tasks, and fetching/processing remote data |
| SI-14 | Skill in operating virtual machines |
| SI-15 | Knowledge of troubleshooting basic systems and operating system related issues |
| SI-16 | Knowledge of operating system structure and internals |
| SI-17 | Skill in utilizing virtual networks for testing |
| SI-18 | Knowledge of operating system's ports and services |
| SI-19 | Skill in installing and configuring virtual machines |
| SI-20 | Skill in matching the appropriate knowledge repository technology for a given application or environment |
| SI-21 | Knowledge of “knowledge base” capabilities in identifying the solutions to less common and more  complex system problems |
| SI-22 | Skill in conducting knowledge mapping |
| SI-23 | Skill in conducting open source research for troubleshooting client-level problems |
| SI-24 | Skill in using knowledge management technologies |
| SI-25 | Knowledge of Storage Area Networks |
| SI-26 | Knowledge of external information system impact to the security baseline |
| SI-27 | Knowledge of information backed up and schedule of information system backup |
| SI-28 | Knowledge of identification and authentication techniques |
| SI-29 | Skills in implementing identification and authentication through various means |
| SI-30 | Knowledge of various types of Spam and other attack methodologies |
| SI-31 | Skill in implementing protective measures for various types of Spam and other attacks |
|  | **IT SYSTEMS AND OPERATIONS** |
| ITOS-1 | Knowledge of circuit analysis |
| ITOS-2 | Knowledge of microprocessors |
| ITOS-3 | Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system |
| ITOS-4 | Knowledge of basic physical computer components and architectures, including the functions of various  components and peripherals (e.g., CPUs, Network Interface Cards, data storage) |
| ITOS-5 | Skill in physically assembling and disassembling PCs |
| ITOS-6 | Skill in conducting information searches |
| ITOS-7 | Skill in the basic operation of computers |
| ITOS-8 | Skill in processing collected data for follow-on analysis |
| ITOS-9 | Knowledge of storage capacity |
| ITOS-10 | Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| ITOS-11 | Knowledge of network hardware devices and functions |
| ITOS-12 | Skill in implementation of auditable events |
| ITOS-13 | Skill in configuring and utilizing hardware-based computer protection components |
| ITOS-14 | Knowledge of electrical engineering as applied to computer architecture, including circuit boards,  processors, chips, and associated computer hardware |
| ITOS-15 | Skill in managing information system accounts and their access to information systems |
| ITOS-16 | Skill in determining organizationally defined auditable events |
| ITOS-17 | Skill in handling audit processing failures |
| ITOS-18 | Knowledge of audit records and the protection thereof |
| ITOS-19 | Skill in implementing the protection of audit records |
| ITOS-20 | Skill in tracking use of software and documentation protected by licenses |
| ITOS-21 | Skill in monitoring policy compliance for user-installed software |
| ITOS-22 | Skill in protecting the confidentiality of transmitted information |
| ITOS-23 | Knowledge that information must be protected at rest and during transmission |
| ITOS-24 | Skill in performing information system backups |
| ITOS-25 | Knowledge of processes to maintain the system and user documentation |
| ITOS-26 | Skill in employing audit reduction and report generation capabilities |
| ITOS-27 | Knowledge of audit reduction and report generation |
|  | **IT SECURITY AWARENESS AND TRAINING** |
| SAT-1 | Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain |
| SAT-2 | Skill in developing curriculum that speaks to the topic at the appropriate level for the target audience |
| SAT-3 | Skill in identifying upcoming IA topics to ensure awareness |
| SAT-4 | Skill in preparing and delivering education and awareness briefings to ensure that systems, network, and  data users are aware of and adhere to systems security policies and procedures |
| SAT-5 | Skill in identifying gaps in technical capabilities |
| SAT-6 | Knowledge of academic institutions dealing with cybersecurity issues |
| SAT-7 | Skill in developing and executing technical training programs and curricula |
| SAT-8 | Skill in maintaining and retaining security training records |
| SAT-9 | Skill in developing and executing tests of the contingency plans |
| SAT-10 | Knowledge of requirements for developer provided IT/cybersecurity training |
| SAT-11 | Skill in training individuals in contingency planning |
| SAT-12 | Skill in training individuals in incident response procedures |
|  | **MANAGEMENT** |
| PM-1 | Knowledge of resource management principles and techniques |
| PM-2 | Knowledge of IT/cybersecurity program management and project management principles and techniques |
| PM-3 | Knowledge of risk management principles |
| PM-4 | Knowledge of budgeting process to ensure security is addressed |
| PM-5 | Skill in the development, implementation and maintenance of systems security plan |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| PM-6 | Skill in the development of security policies and procedures |
| PM-7 | Skill in the implementation of security policies |
| PM-8 | Knowledge of the various security policies and plans |
| PM-9 | Knowledge of external organizations dealing with cybersecurity issues |
| PM-10 | Knowledge of how information needs are translated, tracked, and prioritized across the extended enterprise |
| PM-11 | Knowledge of Privacy Issues and Mitigation |
| PM-12 | Knowledge of federal reporting principles, policies, procedures, and vehicles, including report formats,  reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions |
| PM-13 | Knowledge of the structure and intent of concept operation and rules of engagement |
| PM-14 | Knowledge of the organization's core business/mission processes |
| PM-15 | Knowledge of the risks associated with social media |
| PM-16 | Skill in the measuring and reporting of intellectual capital |
| PM-17 | Knowledge of organization's evaluation and validation requirements |
| PM-18 | Knowledge of established trust relationships with other organizations owning, operating, and/or maintaining external information systems |
| PM-19 | Knowledge that security training records must be retained as well as the retention period |
| PM-20 | Knowledge of organizationally defined auditable events |
| PM-21 | Knowledge of contract agreements and copyright laws for software and associated documentation |
| PM-22 | Knowledge of policies related to user-installed software |
| PM-23 | Skill in understanding the IT Contingency Plan and its associated activities |
| PM-24 | Skill ensuring the information system backup policy is enforced |
| PM-25 | Knowledge of incident response support resources roles |
| PM-26 | Knowledge of incident response plan |
| PM-27 | Knowledge of applicable processes for downgrading media |
| PM-28 | Knowledge of information system security architecture |
| PM-29 | Skill in integrating and supporting information system security architecture |
| PM-30 | Knowledge and understanding of security categorization for information systems |
| PM-31 | Knowledge and understanding information handling and retention policy |
| PM-32 | Knowledge of capital investment with regards to information assurance |
| PM-33 | Skill in developing and implementing appropriate security agreements, such as Memorandum of Agreements, SLAs, etc. |
| PM-34 | Knowledge of Access Control policies, procedures and security controls |
| PM-35 | Knowledge of Contingency Plans and associated guidance |
| PM-36 | Knowledge of Identification and Authentication policies, procedures and security controls |
| PM-37 | Knowledge of Systems Acquisition policies, procedures and associated guidance |
| PM-38 | Knowledge of System and Communications Protection policies, procedures and security controls |
| PM-39 | Knowledge of System Integrity policies, procedures and security controls |
| PM-40 | Knowledge of Audit and Accountability policies, procedures and security controls |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| PM-41 | Knowledge of Incident Response policies, procedures and security controls |
| PM-42 | Knowledge of Maintenance policies, procedures and security controls |
| PM-43 | Knowledge of Maintenance associated guidelines and log implementation |
| PM-44 | Knowledge of Media Protection policies, procedures, associated guidelines and security controls |
| PM-45 | Knowledge of Physical and Environmental policies, procedures and security controls |
| PM-46 | Knowledge of Personnel Security policies, procedures and security controls |
| PM-47 | Knowledge of Security Assessment and Authorization policies, procedures and security controls |
| PM-48 | Knowledge Configuration Management policies, procedures and security controls |
| PM-49 | Knowledge of Risk Management policies, procedures and security controls |
| PM-50 | Knowledge of Security Planning policies, procedures and associated guidelines |
| PM-51 | Knowledge of Security Awareness and Training policies, procedures and associated guidance |
| PM-52 | Knowledge of Return on Investment (ROI) analysis |
| PM-53 | Skill in analyzing return on investment (ROI) |
|  | **MODELING AND SIMULATION** |
| MS-1 | Skill in creating and utilizing mathematical or statistical models |
| MS-2 | Skill in developing data models |
| MS-3 | Skill in the use of design modeling |
|  | **NETWORK AND TELECOMMUNICATIONS SECURITY** |
| NTS-1 | Skill in conducting server planning, management, and maintenance |
| NTS-2 | Skill in correcting physical and technical problems which impact server performance |
| NTS-3 | Skill in diagnosing connectivity problems |
| NTS-4 | Skill in diagnosing failed servers |
| NTS-5 | Skill in testing and configuring network hardware and peripherals |
| NTS-6 | Skill in using network management tools to analyze network traffic patterns |
| NTS-7 | Knowledge of the capabilities of different electronic communication systems and methods |
| NTS-8 | Knowledge of the range of existing networks |
| NTS-9 | Knowledge of network systems management principles, models, methods and tools |
| NTS-10 | Skill in configuring and utilizing network protection components |
| NTS-11 | Knowledge of organization's LAN/WAN pathways and other telecommunication pathways |
| NTS-12 | Knowledge of how network services and protocols interact to provide network communications |
| NTS-13 | Knowledge of local area and wide area networking principles and concepts including bandwidth  management |
| NTS-14 | Knowledge of network protocols |
| NTS-15 | Knowledge of network design processes, to include understanding of security objectives, operational  objectives, and tradeoffs |
| NTS-16 | Knowledge of how traffic flows across the network |
| NTS-17 | Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and  switches |
| NTS-18 | Skill in network mapping and recreating network topologies |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| NTS-19 | Skill in using sub-netting tools |
| NTS-20 | Knowledge of common network tools |
| NTS-21 | Knowledge of host/network access controls |
| NTS-22 | Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins |
| NTS-23 | Knowledge of IT security principles and methods |
| NTS-24 | Knowledge of current industry methods for evaluating, implementing, and disseminating network security  assessment, monitoring, detection and remediation tools and procedures utilizing standards-based concepts and capabilities |
| NTS-25 | Knowledge of network traffic analysis methods |
| NTS-26 | Knowledge of network security design tools, methods, and techniques |
| NTS-27 | Knowledge of the CND Service Provider reporting structure and processes within one’s own organization  for network incidents |
| NTS-28 | Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities |
| NTS-29 | Skill in developing and deploying intrusion detection/protection signatures |
| NTS-30 | Skill in discerning the protection needs (i.e., security controls) of networks |
| NTS-31 | Skill in implementing, maintaining, and improving established network security practices |
| NTS-32 | Knowledge of front-end collection systems, including network traffic collection, filtering, and selection |
| NTS-33 | Knowledge of security event correlation tools |
| NTS-34 | Knowledge of current and emerging threats/threat vectors |
| NTS-35 | Knowledge of basic network administration, and network hardening techniques |
| NTS-36 | Knowledge of network security architecture concepts including topology, protocols, components, and  principles |
| NTS-37 | Skill in reading and interpreting intrusion detection/protection signatures |
| NTS-38 | Knowledge of intrusion detection/protection signature implementation impact |
| NTS-39 | Skill in enforcement of policies |
| NTS-40 | Knowledge of packet-level analysis |
| NTS-41 | Knowledge of telecommunications concepts |
| NTS-42 | Knowledge of basic concepts, terminology, and operations of a wide range of communications media |
| NTS-43 | Knowledge of different types of network communication |
| NTS-44 | Knowledge of the nature and function of the relevant information structure |
| NTS-45 | Knowledge of Voice over IP (VoIP) |
| NTS-46 | Knowledge of mobile communications architecture |
| NTS-47 | Knowledge of transmission methods |
| NTS-48 | Skill in establishing a routing schema |
| NTS-49 | Skill in applying network programming towards client/server model |
| NTS-50 | Knowledge of organization's LAN/WAN pathways |
| NTS-51 | Skill in testing alternate telecommunication services |
| NTS-52 | Knowledge of collaborative computing devices and their risk to the information system security baseline |
|  | **PERSONNEL SECURITY** |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| PS-1 | Knowledge of human-computer interaction principles |
| PS-2 | Knowledge of and promotion of general awareness regarding the use of social engineering techniques |
| PS-3 | Knowledge of Privacy Impact Assessments |
| PS-4 | Knowledge of operations security |
| PS-5 | Skill in assigning position descriptions |
| PS-6 | Knowledge of hiring, termination, and transfer actions impacting information systems access |
| PS-7 | Knowledge of third party access requirements |
| PS-8 | Knowledge of ethical testing |
| PS-9 | Knowledge of social dynamics of computer attackers in a global context |
| PS-10 | Knowledge of threat list countries’ cyber capabilities, intent, opportunities, and presence |
| PS-11 | Knowledge of correct behavior for information system use |
| PS-12 | Skill in writing the rules that govern correct behavior for information system use |
|  | **PHYSICAL AND ENVIRONMENTAL SECURITY** |
| PES-1 | Knowledge of physical access controls |
| PES-2 | Skill in implementing various physical access controls |
| PES-3 | Skill in monitoring physical access |
| PES-4 | Knowledge of emergency power |
| PES-5 | Knowledge of fire protection systems |
| PES-6 | Knowledge of environmental controls and hazards |
| PES-7 | Skill in configuring ports and input/output devices |
| PES-8 | Knowledge of physical controls for datacenter(s) |
| PES-9 | Skill in implementing physical controls for areas housing computer systems and networks |
|  | **PROCUREMENT** |
| PROC-1 | Knowledge of applicable business processes and operations of customer organizations |
| PROC-2 | Knowledge of capabilities and requirements analysis |
| PROC-3 | Knowledge of system software and organizational design standards, policies, and authorized approaches relating to system design |
| PROC-4 | Skill in conducting capabilities and requirements analysis |
| PROC-5 | Skill in interpreting and translating customer requirements into operational cyber actions |
| PROC-6 | Knowledge of secure acquisitions |
| PROC-7 | Knowledge of Export Control regulations and responsible Federal Organizations for the purposes of  reducing supply chain risk |
| PROC-8 | Knowledge of critical IT procurement requirements |
| PROC-9 | Knowledge of functionality, quality, and security requirements and how these will apply to specific items  of supply (i.e., elements and processes) |
| PROC-10 | Skill in evaluating the trustworthiness of the supplier and/or product |
| PROC-11 | Knowledge of processes to allocate resources in business process planning |
| PROC-12 | Skill in ensuring the proper allocations of resources in business process planning |
|  | **SECURITY RISK MANAGEMENT** |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| RM-1 | Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems |
| RM-2 | Skill to identify systemic security issues based on the analysis of vulnerability and configuration data |
| RM-3 | Knowledge of application vulnerabilities |
| RM-4 | Knowledge of penetration testing principles, tools, and techniques |
| RM-5 | Knowledge of system and application security threats and vulnerabilities |
| RM-6 | Knowledge of network security threats and vulnerabilities |
| RM-7 | Skill in assessing the robustness of security systems and designs |
| RM-8 | Skill in designing countermeasures to identified security risks |
| RM-9 | Skill in evaluating the adequacy of security designs |
| RM-10 | Skill in performing packet-level analysis |
| RM-11 | Skill in the use of penetration testing tools and techniques |
| RM-12 | Skill in using protocol analyzers |
| RM-13 | Skill in applying white hat hacking/security auditing techniques, procedures, and tools |
| RM-14 | Skill in using network analysis tools to identify vulnerabilities |
| RM-15 | Skill in utilizing exploitation tools to identify system/software vulnerabilities |
| RM-16 | Skill in utilizing network analysis tools to identify software communications vulnerabilities |
| RM-17 | Knowledge of reverse engineering concepts and techniques |
| RM-18 | Knowledge of how different file types can be used for anomalous behavior |
| RM-19 | Knowledge of measures or indicators of system performance and availability |
| RM-20 | Knowledge of performance tuning tools and techniques |
| RM-21 | Skill in identifying and anticipating server performance, availability, capacity, or configuration problems |
| RM-22 | Skill in identifying measures or indicators of system performance and the actions needed to improve or  correct performance relative to the goals of the system |
| RM-23 | Skill in monitoring and optimizing server performance |
| RM-24 | Skill in conducting audits or reviews of technical systems |
| RM-25 | Skill in risk management processes, including steps and methods for assessing risk |
| RM-26 | Knowledge of organization's risk tolerance and/or risk management approach |
| RM-27 | Knowledge of supply chain risk management processes and practices |
| RM-28 | Knowledge of risk threat assessment |
| RM-29 | Skill in implementing IT supply chain security/risk management policies, requirements, and procedures |
| RM-30 | Knowledge of Risk Management Framework |
| RM-31 | Skill in creating policies that reflect system security goals |
| RM-32 | Skill in correlation of data to develop information about the capabilities, intent, and operations of criminal  and/or adversary organizations |
| RM-33 | Knowledge of hacking methodologies |
| RM-34 | Skill in analyzing audit records |
|  | **SOFTWARE** |
| SW-1 | Knowledge of software debugging principles |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
| SW-2 | Knowledge of software design tools, methods, and techniques |
| SW-3 | Skill in conducting software debugging |
| SW-4 | Skill in developing applications that can log errors, exceptions, and application faults and logging |
| SW-5 | Skill in using code analysis tools to eradicate bugs |
| SW-6 | Skill in writing kernel level applications |
| SW-7 | Knowledge of Middleware |
| SW-8 | Knowledge of debugging procedures and tools |
| SW-9 | Skill in developing technical design documentation |
| SW-10 | Skill in developing software design documentation |
| SW-11 | Knowledge of software development models |
| SW-12 | Knowledge of software engineering |
| SW-13 | Skill in configuring and optimizing software |
| SW-14 | Knowledge of software quality assurance process |
| SW-15 | Knowledge of secure software deployment methodologies, tools and practices |
| SW-16 | Skill in configuring and utilizing software-based computer protection tools |
| SW-17 | Skill in creating programs that validate and process multiple inputs including command line arguments,  environmental variables, and input streams |
| SW-18 | Skill in tailoring code analysis for application-specific concerns |
| SW-19 | Knowledge of low-level computer languages |
| SW-20 | Knowledge of programming language structures and logic |
| SW-21 | Skill in writing code in a modern programming language |
| SW-22 | Knowledge of language command line(s) |
| SW-23 | Knowledge of interpreted and compiled computer language |
| SW-24 | Knowledge of secure coding techniques |
| SW-25 | Skill in using binary analysis tools |
| SW-26 | Skill in reading Hexadecimal data |
| SW-27 | Skill in identifying common encoding techniques |
| SW-28 | Knowledge of system security plans |
| SW-29 | Skill in the implementation of security plans |
| SW-30 | Knowledge of software, firmware, and information integrity verification tools |
| SW-31 | Skill in employing software, firmware, and information integrity verification tools |
| SW-32 | Knowledge of software assurance |
|  | **SYSTEMS AND APPLICATION SECURITY** |
| SAS-1 | Knowledge of server administration and systems engineering theories, concepts, and methods |
| SAS-2 | Knowledge of systems lifecycle management principles, including software security and usability |
| SAS-3 | Knowledge of the operations and processes for diagnosing common or recurring system problems |
| SAS-4 | Knowledge of the systems engineering process |
| SAS-5 | Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning |

|  |  |
| --- | --- |
| **K&S ID** | **Knowledge and Skills** |
|  | properly |
| SAS-6 | Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation |
| SAS-7 | Skill in installing computer and server upgrades |
| SAS-8 | Knowledge of the life cycle process |
| SAS-9 | Knowledge of systems diagnostic tools and fault identification techniques |
| SAS-10 | Knowledge of systems testing and evaluation methods |
| SAS-11 | Skill in applying organization-specific systems analysis principles and techniques |
| SAS-12 | Skill in conducting test events |
| SAS-13 | Skill in designing a data analysis structure |
| SAS-14 | Skill in determining an appropriate level of test rigor for a given system |
| SAS-15 | Skill in developing operations-based testing scenarios |
| SAS-16 | Skill in systems integration testing |
| SAS-17 | Skill in writing test plans |
| SAS-18 | Skill in evaluating test plans for applicability and completeness |
| SAS-19 | Skill in secure test plan design |
| SAS-20 | Knowledge of known system and application vulnerabilities from alerts, advisories, errata, and bulletins |
| SAS-21 | Knowledge of IT/cybersecurity systems engineering principles |
| SAS-22 | Knowledge of system and application security principles and methods |
| SAS-23 | Knowledge of current industry methods for evaluating, implementing, and disseminating IT security assessment, monitoring, detection and remediation tools and procedures utilizing standards-based concepts  and capabilities |
| SAS-24 | Knowledge of security system design tools, methods, and techniques |
| SAS-25 | Knowledge of the Service Provider reporting structure and processes within one’s own organization |
| SAS-26 | Skill in discerning the protection needs (i.e., security controls) of information systems |
| SAS-27 | Knowledge of system and application security event correlation tools |
| SAS-28 | Knowledge of software related IT security principles and methods |
| SAS-29 | Knowledge of basic system administration, and operating system hardening techniques |
| SAS -30 | Skill in basic system administration, and operating system hardening techniques |
| SAS-31 | Knowledge of signature implementation impact |
| SAS-32 | Knowledge of malicious code protection mechanisms |
| SAS-33 | Skill in implementing malicious code protection |
| SAS-34 | Knowledge of current and emerging threats/threat vectors against information systems and applications |

# Appendix C: Roles

This Appendix is designed to assist in determining which competency and associated Knowledge and Skills are required by a particular role. Knowledge is the theoretical or practical understanding of the competency.

Please note that there is no hierarchy within the Knowledge and Skills. No Knowledge or Skill is of greater value than another. The first Knowledge and Skill listed within the knowledge unit has no order preference on those Knowledge and Skills listed elsewhere in list.

Additionally, the generic roles and job titles used within this Appendix may or may not be the same as the roles or job titles used by and individual Agency or organization. The ones used within this Appendix are a sample of current jobs/roles within various Federal Organizations and organizations at the time of publication. Using the competencies and functions, each of these samples can be tailored to meet the roles within a specific Agency.

Roles for highly specialized areas are not covered. The roles, and associated knowledge and skills should be tailored by the Agency.

All roles should have training on the Overall Knowledge and Skills as described within Appendix C, Competencies, Knowledge and Skills Catalog. These are the fundamental basis of knowledge/skills required for all jobs and roles.

Abilities are not covered in this document. Abilities are the specific skills that are obtained while on the job using the knowledge and skills that were obtained during the role-based security training. Therefore, it is assumed that abilities cannot be taught, but rather acquired throughout the employee’s career.

The format is as follows:

* **Function Area**: This area corresponds with *Appendix A: Function Areas*. Appendix A provides a general description of the area and the Learning Objectives for those functions. The roles described within this appendix are within a function;
* **Role Area**: This describes the overall role;
* **Roles**: A list of various job title /roles is provided to assist in determining who should receive this role based training;
* **Responsibility**: Defines the activities and or responsibilities of that particular role;
* **Knowledge Unit**: Identifies the competencies associated with the role. The entire listing of the knowledge units and their associated knowledge and skills are located in *Appendix B: Knowledge and Skills Catalog*; and
* **Corresponding Knowledge and Skills Table**: This table provides a breakdown of the specific knowledge unit, the corresponding knowledge and skills to each competency. Each role has various knowledge units associated with it. There are 4 differing functional perspectives that

correspond with the job title to allow for further tailoring of role-based training to better match with the job role. These areas are defined as follows:

* + **Manage** – those knowledge and skills particular to those employees who are responsible for management (e.g., managers, team leads, project managers)
  + **Design** – those knowledge and skills particular to those employees who are responsible for design activities (e.g., system developers, engineers)
  + **Implement** – those knowledge and skills particular to those employees who execute implementation (e.g., system administrators, network administrators)
  + **Evaluate** – those knowledge and skills particular to evaluation activities (e.g., testers, security analysts)

To assist with the tailoring of the training or to identify courses/modules that may have already been developed, there is the National Initiative for Cybersecurity Careers and Studies (NICCS) Portal. The government developed the National Initiative for Cybersecurity Careers and Studies (NICCS) to make cybersecurity information and materials more readily-available. NICCS underscores the four components of the National Initiative for Cybersecurity Education (NICE) and serves as a national resource for government, industry, academia, and the general public in their quest to learn about cybersecurity awareness, education, careers, and workforce development opportunities. The portal links to various courses or modules in cybersecurity that have been previously developed and can be reused. The URL is: [http://niccs.us-cert.gov](http://niccs.us-cert.gov/)

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Operate and Maintain

**Role Area**: Data Administration

###### Roles:

* Data Security Analyst
* Data Management Systems Security
* Data Administrator
* Database Administrator
* Content Staging Specialist
* Data Architect
* Data Manager
* Data Warehouse Specialist
* Database Developer
* Information Dissemination Manager
* Information System Integrator

**Responsibility** — Develop and administer databases and/or data management systems that allow for the storage, query, and utilization of data.

###### Knowledge Unit:

* Data Security
* Digital Forensics
* Database
* Cryptography and Encryption
* Architecture
* Identity Management/Privacy
* Information Systems
* Modeling and Simulation
* Incident Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Data Security** | DS-2 DS-10 DS-18 | DS-4 | DS: 3 -8  DS: 13 - 14  DS: 16 | DS: 3 - 6 DS-9  DS-12 DS: 17-18 | DS-9 DS-11 DS-13 DS-15 DS: 17-18 |
| **Digital Forensics** |  |  |  | DF-6 | DF-7 DF-31 |
| **Database** |  | DB-5 | DB-1 DB-2  DB-4 DB-6 | DB-3 DB: 7 - 8  DB: 9 - 11 |  |
| **Cryptography and Encryption** |  | CR-10 CR-12 | CR-1 CR-5 | CR-3 CR-5 CR-7 | CR-9 |
| **Architecture** |  | ARCH-15 | ARCH-2 ARCH-7 ARCH: 18 – 21 | ARCH-1 ARCH-3 ARCH-4 ARCH-9 |  |
| **Identity Management**  **/Privacy** | IM: 1-3 IM-7 | IM-9 IM-11 | IM-5 | IM: 4-6 IM-9 | IM-4 IM-5  IM-8 IM-10 IM-11 |
| **Information Systems** | SI: 1-3 SI-10  SI: 27 -28 SI-30 | SI-25 | SI-4 SI-5  SI-9 SI-13  SI-25 SI-29 | SI-5 SI-7  SI-8 SI-9 SI: 14 - 15  SI-20 SI-25 SI-29 SI-31 | SI-17 SI-26 SI- 31 |
| **Modeling and Simulation** |  |  | MS: 2 – 3 |  |  |
| **Incident Management** | IR-20 | IR-2 IR-3 IR-6 IR-14 IR-16 IR- 18 |  | IR-4 IR-12 | IR: 2 - 3 IR-14 |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Operate and Maintain

**Role Area**: Knowledge Management

###### Roles:

* Freedom of Information Act Official
* Information Owner/Steward
* Information Resource Manager
* Web Administrator
* Business Intelligence Manager
* Content Administrator
* Document Steward
* Information Manager
* Information Security Architect

**Responsibility** — Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

###### Knowledge Unit:

* Information Systems
* Network and Telecommunications Security
* Emerging Technology
* Data Security
* IT Systems and Operations
* Incident Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
| **Information Systems** |  | SI-24 | SI: 1-3 SI-22 | SI: 1 - 4  SI: 7 - 8 SI-13  SI-22 SI-24 |  |
| **Network and Telecommunications**  **Security** | NTS-22 NTS-23 | NTS-9 NTS-44 |  | NTS-9 NTS-34  NTS-44 |  |
| **Emerging Technology** | ET-1 ET-11 | ET: 3 - 4 ET-6  ET-8 ET-10 | ET-3 ET-5 | ET: 3 - 5 |  |
| **Data Security** |  | DS-2 DS-4 DS-18 | DS-2 DS-5 DS: 7 - 8  DS-10 DS-13  DS-15 | DS-2 DS: 4 - 5  DS: 7 - 10 DS-18 |  |
| **IT Systems and Operations** |  | ITOS-15 ITOS: 21 - 23 | ITOS-4 | ITOS-6 ITOS-8 ITOS-20  ITOS: 22 - 24 ITOS-27 | ITOS-8 |
| **Incident Management** | IR-20 | IR: 1 - 2  IR-16 |  |  |  |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Operate and Maintain

**Role Area**: Customer Service and Technical Support

###### Roles:

* Service Desk Representative
* Service Desk Operator
* Technical Support Personnel
* System Administrator
* Helpdesk Representative
* Customer Support Specialist
* Customer Support
* System Evaluator

**Responsibility** — Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

###### Knowledge Unit:

* Information Systems
* Incident Management
* Security Risk Management
* Systems and Applications Security
* Network and Telecommunications Security
* IT Systems and Operations

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Information Systems** | SI: 1 - 3 | SI-11 |  | SI: 8 - 16 SI: | SI: 8 – 17 |
|  | SI: 5– 7 | SI-18 | 18 - 19 SI-25 | SI-19 |
|  |  |  | SI: 28 - 30 | SI-23 |
|  |  |  |  | SI: 28 - 29 |
| **Incident Management** | IR-1 |  |  |  |  |
|  | IR-6 |
|  | IR-16 |
|  | IR-18 |
|  | IR-20 |
| **Security Risk** | RM-3 | RM: 25 - 26 |  | RM: 20 - 23 |  |
| **Management** | RM: 5 - 6 | RM-28 |  |
|  | RM-19 |  |  |
| **Systems and Applications** |  | SAS-8 |  | SAS: 1 - 2 | SAS-3 |
| **Security** | SAS-20 | SAS: 5 - 7 | SAS-6 |
|  | SAS-22 | SAS: 29 - 30 | SAS: 9 - 10 |
|  | SAS-25 | SAS: 32 - 33 |  |
|  | SAS: 27 - 29 |  |  |
| **Network and** |  | NTS-9 |  | NTS: 1 - 6 | NTS: 3 - 4 |
| **Telecommunications** | NTS: 22 - 23 | NTS: 8 - 14 | NTS-6 |
| **Security** | NTS: 27 - 28 | NTS: 16 - 21 | NTS-17 |
|  | NTS-35 | NTS-25 | NTS-51 |
|  | NTS: 41 - 42 | NTS-35 |  |
|  |  | NTS: 41 - 43 |  |
|  |  | NTS-45 |  |
|  |  | NTS-47 |  |
|  |  | NTS-50 |  |
| **IT Systems and** |  | ITOS: 3 - 4 ITOS-7 |  | ITOS: 2 - 5 |  |
| **Operations** |  | ITOS-7 |
|  |  | ITOS: 10 - 11 |
|  |  | ITOS-13 ITOS-20 |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Operate and Maintain

**Role Area**: Network Services

###### Roles:

* Network Administrator
* Telecommunication Personnel
* Network Security Specialist
* Telecommunication Engineer
* Continuous Monitoring Executer
* Cabling Technician
* Converged Network Engineer
* Network Analyst
* Network Designer
* Network Engineer
* Network Systems and Data Communications Analyst
* Enterprise Architect
* Information Security Architect
* Information System/Security Engineer
* Information System Integrator
* System Evaluator

**Responsibility** — Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

###### Knowledge Unit:

* Architecture
* IT Systems and Operations
* Information Assurance
* Information Systems
* Network and Telecommunications Security
* Security Risk Management
* Systems and Applications Security
* Cryptography and Encryption
* Data Security
* Configuration Management
* Computer Network Defense
* Web Technology
* Identity Management/Privacy
  + Incident Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Architecture** | ARCH: 10 - 12 | ARCH-5 ARCH-8 | ARCH: 1 - 3 | ARCH: 1 - 9 | ARCH: 1 - 3 |
|  | ARCH-15 |  | ARCH: 5 - 9 ARCH: | ARCH: 13- 14 ARCH: | ARCH: 8 - 9 |
|  | ARCH: 18 - 19 |  | 13 -14 | 16 - 17 ARCH-20 | ARCH-14 ARCH-17 |
|  |  |  | ARCH-21 |  | ARCH: 20 - 21 |
| **IT Systems and Operations** | ITOS-4 | ITOS: 15 - 16 | ITOS: 1 - 2 | ITOS: 1 - 3 | ITOS-3 |
|  | ITOS-7 | ITOS-27 | ITOS-10 | ITOS: 5 - 6 | ITOS-6 |
|  | ITOS-11 |  | ITOS: 13 - 14 ITOS- | ITOS: 8 - 10 | ITOS-8 |
|  | ITOS-18 |  | 16 | ITOS: 12 - 17 | ITOS-10 |
|  | ITOS-23 |  | ITOS-22 | ITOS: 19 - 22 | ITOS: 14 - 15 |
|  | ITOS-25 |  |  | ITOS-24 | ITOS-17 |
|  |  |  |  | ITOS: 26 - 27 | ITOS: 20 - 21 |
|  |  |  |  |  | ITOS: 26 - 27 |
| **Information Assurance** | IA-9 | IA: 1 - 5 | IA-3 | IA: 6 - 8 | IA: 1 - 2 |
|  |  |  | IA: 6 - 7 |  | IA-4 |
|  |  |  |  |  | IA: 7 - 8 |
| **Information Systems** | SI: 2 - 3 | SI-7 | SI-1 | SI-1 | SI-11 |
|  | SI: 5 - 6 | SI-21 | SI-4 | SI: 7 - 15 | SI-13 |
|  | SI-16 | SI: 26 - 27 SI-30 | SI: 9 – 12 | SI: 18 - 20 | SI-15 |
|  | SI-28 |  | SI-18 | SI: 22 - 25 | SI: 17 - 18 |
|  |  |  | SI: 20 - 22 | SI-27 | SI-23 |
|  |  |  | SI-25 | SI-29 | SI: 26 - 27 |
|  |  |  | SI-27 | SI: 30-31 | SI: 29 - 31 |
|  |  |  | SI-29 |  |  |
|  |  |  | SI-31 |  |  |
| **Network and** | NTS: 7 - 9 | NTS-24 | NTS-1 | NTS: 1 - 6 | NTS: 3 - 6 |
| **Telecommunications** | NTS: 11 - 16 | NTS: 27 - 28 | NTS-26 | NTS-10 | NTS-10 |
|  | NTS: 20 - 23 | NTS-30 | NTS-46 | NTS: 17 – 19 | NTS-17 |
|  | NTS-25 | NTS-33 | NTS-48 | NTS: 27 - 33 | NTS-24 |
|  | NTS: 34 - 36 | NTS: 38 - 39 NTS- | NTS-52 | NTS-38 | NTS: 27 - 28 |
|  | NTS: 41 - 45 | 52 |  | NTS-40 | NTS: 30- 33 |
|  | NTS-47 |  |  | NTS: 48 - 49 | NTS-37 |
|  | NTS-50 |  |  |  | NTS: 39-40 |
|  |  |  |  |  | NTS-51 |
| **Security Risk Management** | RM-6 | RM: 25 - 26 | RM: 7 - 8 | RM: 1 - 2 | RM: 1 - 2 |
|  |  | RM-28 | RM-18 | RM-10 | RM-4 |
|  |  | RM: 30-31 |  | RM-12 | RM-7 |
|  |  |  |  | RM-14 | RM: 9 - 10 |
|  |  |  |  | RM-16 | RM: 12 - 14 |
|  |  |  |  | RM-18 | RM-16 |
|  |  |  |  | RM-20 | RM-18 |
|  |  |  |  | RM-22 | RM-25 |
|  |  |  |  | RM: 33 - 34 | RM: 32 - 33 |
| **Cryptography and** | CR-1 CR-3 CR-10 | CR-10 | CR-2 | CR: 4 - 5 | N/A |
| **Encryption** |  | CR-12 | CR: 4 - 5 | CR: 11 - 12 |  |
|  |  | CR-14 | CR-12 | CR-15 |  |
| **Data Security** | N/A | DS-4 | DS-2 | DS: 1 - 2 | N/A |
|  |  | DS-18 |  | DS-4 |  |
|  |  |  |  | DS-15 |  |
|  |  |  |  | DS-18 |  |
| **Configuration Management** | CM-1 | CM-7 | CM-13 | CM: 2 - 3 | CM-4 |
|  | CM: 5 - 6 | CM-12 |  | CM-8 |  |
|  | CM-9 | CM-15 |  | CM-10 |  |
|  | CM-11 |  |  | CM-12 |  |
|  |  |  |  | CM-14 |  |
| **Computer Network Defense** | CND: 1 - 2 CND-11 | CND-4 | CND-12 | CND: 4 - 5 | CND: 5 - 6 |
|  | CND: 17 - 20 CND- | CND: 9 -10 CND- |  | CND-8 | CND-10 |
|  | 22 | 12 |  | CND: 14 - 16 | CND-13 |
|  |  | CND: 14 - 16 |  | CND-28 | CND-21 |
|  |  | CND: 29 - 30 |  |  | CND: 24 - 29 |
| **Web Technology** | WT-1 | N/A | N/A | WT-9 | N/A |
| **Identify Management/** | IM: 1 – 3 | N/A | N/A | IM: 4 - 6 | N/A |
| **Privacy** | IM-7 |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
| **Incident Management** | IR: 1 - 3 |  |  | IR: 9- 10 | IR: 12 - 15 |
|  | IR-6 | IR-12 |  |
|  | IR-16 | IR-17 |  |
|  | IR-18 |  |  |
|  | IR-20 |  |  |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Operate and Maintain **Role Area**: System Administration **Role**:

* Directory Services Administrator
* System Administrator
* Operations Personnel/Management
* LAN administrator
* Platform Specialist
* Security Administrator
* Systems Operations Personnel
* Server Administrator
* Website Administrator
* Information Security Architect
* Information Security Integrator

**Responsibility** — Installs, configures, troubleshoots and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control/passwords/account creation and administration.

###### Knowledge Unit:

* Information Systems
* Network and Telecommunications Security
* Architecture
* Security Risk Management
* Emerging Technologies
* Systems and Applications Security
* Digital Forensics
* Cryptography and Encryption
* Software
* Identity Management/Privacy
* Incident Management
* Configuration Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Information Systems** | SI-3 SI-5  SI: 6 - 8 SI-10 SI-26 SI-28  SI-30 | SI-10 SI-20 SI-25 | SI: 1 - 2 SI-4  SI: 9 - 10 SI-16  SI-18  SI: 20 - 21 | SI: 1 – 2  SI: 9 - 16  SI: 18 - 19 SI-23  SI-27 SI-29 SI-31 | SI-1  SI: 11 – 13  SI: 15 - 17 SI-21  SI-23 SI-31 |
| **Network and Telecommunication s Security** | NTS-1 NTS-7 NTS-22 NTS-24 NTS-35  NTS-52 | NTS-23 NTS-39 | N/A | NTS-2 NTS: 4 - 5 NTS-23  NTS: 38 - 39 | NTS: 2 - 6 NTS-23 |
| **Architecture** | ARCH - 3 ARCH-14 ARCH-18 | ARCH-2 ARCH-8 ARCH-13  ARCH-15 | ARCH-1 ARCH: 4 - 6 ARCH-21 | ARCH: 1 - 2 ARCH-4 ARCH-6 | ARCH-21 |
| **Security Risk Management** | RM-3 RM-5 RM-19 RM-21 RM-30 | RM-2  RM: 25 - 28 RM-31 | RM-8 RM-18 | RM-1 RM-8 RM-18 RM-20  RM: 23 - 24 RM-34 | RM-1 RM-7  RM: 22 - 23 RM-34 |
| **Emerging Technologies** | ET: 1 – 2  ET: 8 - 11 | ET-7 | N/A | ET-4 | N/A |
| **Systems and Applications Security** | SAS: 1 – 3 SAS-8 SAS-11 SAS-20  SAS: 22 - 23  SAS: 29 - 30 | SAS-25 SAS-27 | SAS-4 SAS-24 SAS-26 | SAS: 5 - 7 SAS-16 SAS: 25 - 26  SAS: 30 - 31 | SAS-6 SAS: 9 - 10 SAS-16  SAS: 25 - 27  SAS: 30 - 31 |
| **Digital Forensics** | DF-1 | DF-6 | N/A | DF: 6 – 7  DF-11 | DF-7  DF-11 |
| **Cryptography and Encryption** | CR-1 CR-5 CR-10  CR-12 | N/A | CR-2 | CR-11 CR-13 | N/A |
| **Software** | SW-9 SW-19 SW-21 SW-28  SW-30 | SW-15 | SW-7 SW-17  SW: 21 - 23 SW-29  SW-32 | SW: 7 – 8  SW: 15 - 16 SW-18  SW: 22 - 23 SW-29 | SW-8 SW-15 SW-22 SW-29 |
| **Identity**  **Management/Priva cy** | IM-1 IM-3  IM-7 IM-9 | N/A | IM-5 | IM: 4 - 6 IM-8 | IM-8 IM-11 |
| **Incident Management** | IR: 1- 3 IR-6  IR-11 IR-20 | N/A | N/A | IR: 4 - 5 IR-9  IR-12 | IR: 7 - 9 |
| **Configuration Management** | CM: 1 – 2  CM: 5 – 6 CM-11 | CM-7 CM: 9 - 10 CM-12  CM: 14 - 15 | N/A | CM-3 CM: 8 - 10  CM: 14 - 15 | CM-9 |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Operate and Maintain **Role Area**: Systems Security Analysis **Roles**:

* IT/cybersecurity Officer
* Information Systems Security Officer
* Security Control Assessor
* Blue/Red Teams
* Penetration Tester
* Platform Specialist
* Security Administrator
* IA Operational Engineer
* IT/cybersecurity Analyst/Administrator/Manager
* Common Control Provider
* Information System Security Engineer
* Penetration Tester
* Independent Verifiers/Validators

**Responsibility** — Conducts the integrations/testing, operations, and maintenance of systems security.

###### Knowledge Unit:

* Security Risk Management
* IT Security Awareness and Training
* Cryptography and Encryption
* Database
* IT Systems and Operations
* Architecture
* Information Assurance
* Information Systems
* Personnel Security
* Network and Telecommunication Security
* Identity Management/Privacy
* Configuration Management
* Software
* Systems and Applications Security
* Incident Management
* Procurement
* Compliance

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Security Risk Management** | RM-3  RM: 5 - 6 RM-18 RM-33 | RM: 25 - 31 | RM-9 RM-17 | RM: 1 - 2 RM-8  RM: 19 - 24 RM-29 | RM: 1 – 2 RM-4 RM-7  RM: 9 – 16  RM: 21 - 22  RM: 32 RM-34 |
| **IT Security Awareness and Training** | N/A | SAT-3  SAT: 5 - 6 SAT-8 | N/A | N/A | SAT: 9 - 10 |
| **Cryptography and Encryption** | N/A | N/A | N/A | N/A | CR: 1 - 5 CR-8 CR-10  CR-12 |
| **Database** | N/A | N/A | DB-2 | DB: 10 - 11 | DB: 4 - 7 |
| **IT Systems and Operations** | ITOS-7 ITOS: 10 -11 | ITOS-16 ITOS-21 ITOS-23 ITOS-25  ITOS-27 |  | ITOS: 12 - 13 ITOS-15 ITOS: 18 - 21 ITOS-24  ITOS-26 | ITOS: 1 - 2  ITOS: 4 – 6 ITOS-8 ITOS: 17 - 19 |
| **Architecture** | ARCH: 18 - 20 | ARCH-2 ARCH-15 | N/A | N/A | ARCH: 2 - 4 ARCH-17  ARCH-21 |
| **Information Systems** | N/A | SI-26 | SI-26 | SI-27 | SI: 17 - 18  SI- 22  SI: 27 - 28  SI: 30 - 31 |
| **Personnel Security** | N/A | PS: 1 - 4 PS-8  PS: 10 - 12 | N/A | PS-4 PS-11 | PS: 8 - 9 |
| **Network and Telecommunication Security** | N/A | NTS: 22 - 24  NTS: 27 - 28 NTS-31 NTS: 33 - 34 NTS-52 | N/A | NTS-31 NTS-35 NTS-39 NTS-52 | NTS-6 NTS: 8 - 9  NTS: 16 - 17  NTS: 20 - 26  NTS: 28 - 30  NTS: 33 - 34  NTS: 36 - 38  NTS: 40 - 47  NTS: 51 - 52 |
| **Identity Management/Privacy** | IM: 7 - 8 | IM-3  IM: 9 – 10 | N/A | IM-5  IM-11 | IM: 1 - 3  IM: 10 - 11 |
| **Information Assurance** | IA: 1 – 2  IA-4 | IA-5 | IA-3  IA-6 | IA-8 | IA-7  IA-9 |
| **Configuration Management** | N/A | CM-1 CM-7 CM-9  CM: 11 - 12 | N/A | CM-2 CM-8 CM-10 | CM-4 |
| **Software** | N/A | SW: 28 - 29 SW-32 | N/A | SW-29 | SW: 24 - 28  SW: 30 – 32 |
| **Systems and Applications Security** | SAS-4 | SAS-20 SAS-25 SAS-34 | N/A | SAS-30 SAS-33 | SAS-2 SAS-10  SAS-12 SAS-14 SAS: 15 - 24  SAS: 26 - 29 SAS-32  SAS-34 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
| **Incident Management** | IR-18 | IR: 1 - 3 IR-6  IR-13 IR-16 IR-20 | N/A | IR: 2 - 3  IR: 11-12 IR-19 | IR-1 IR-3 IR-5  IR: 7 - 10  IR: 13 - 17  IR: 19 - 20 |
| **Procurement** | N/A | PROC: 5 - 8 | N/A | N/A | N/A |
| **Compliance** | N/A | COMP: 1 - 10 | N/A | N/A | COMP-8 |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Securely Provision/Development

**Role Area**: Information Assurance Compliance

###### Roles:

* Accreditor
* Auditor
* Authorizing Official Designated Representative
* Certification Agent
* Certifying Official
* Designated Accrediting Authority
* Compliance Officer/Manager
* Compliance Analyst/Manager
* IA Manager
* IA Officer
* Mission/Business Owner
* Portfolio Manger
* Risk/Vulnerability Manager
* Security Control Assessor
* Independent Verifier/Validator
* Inspector General
* Inspector/Investigator
* Regulatory Affairs Analyst
* IT Security Program Manager
* Governance Manager

**Responsibility** — Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization’s IA requirements. Ensures compliance from internal and external perspectives.

###### Knowledge Unit:

* Computer Network Defense
* Information Systems
* Network and Telecommunications Security
* Information Assurance
* Systems and Applications Security
* Emerging Technology
* Architecture
* Security Risk Management
* Incident Management
* Identity Management/Privacy

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **CND** | CND-1 CND-4 CND-11 CND-15 CND-20 CND-22 | CND-9 CND: 17 - 18 CND-29 CND-30 | CND-3 CND-12 CND-14 CND-16 | CND-2 CND-5 CND-8  CND: 13 - 14 CND-16 CND-19 CND-23 CND-29 | CND-2 CND: 5 - 7 CND-10 CND-13 CND-15 CND-17 CND-19 CND-21  CND: 24 – 29 |
| **Information Systems** | SI-3  SI: 5 - 8 SI-10 SI-26 SI-28 SI-30 | SI-10 SI-20 SI-25 | SI: 1 - 2 SI-4  SI: 9 - 10 SI-16  SI-18  SI: 20 - 21 | SI : 1 - 2  SI: 9 - 16  SI: 18 - 19 SI-23  SI-27 SI-29 SI-31 | SI-1 SI:11 - 13  SI: 15 - 17 SI-21  SI-23 SI-31 |
| **Network and Telecomm Security** | NTS-7 NTS-11 NTS: 14-15 NTS:21-22 NTS-24 NTS-31 | NTS-9 NTS-16 NTS-23 NTS-28 NTS-35 NTS:38-39 NTS-52 | N/A | NTS-26 NTS-29 NTS-32 NTS-52 | NTS-8  NTS: 11 - 12  NTS: 16 - 17 NTS-19 NTS-23 NTS: 27 - 29 NTS-32 NTS: 37 - 40  NTS: 51 - 52 |
| **Information**  **Assurance** | IA-1 | IA: 2 - 5  IA-9 | IA-3 IA-6 | IA: 7 - 8 | IA-2  IA: 7 - 9 |
| **Sys and App Security** |  | SAS-10 SAS-12 SAS: 17 - 18 SAS-20 SAS: 25 - 27 |  | SAS: 14 - 16 | SAS-6 SAS: 9 - 10 SAS-12  SAS: 14 - 19 SAS-23 SAS: 26 - 27 |
| **Emerging Technology** | ET-1 | ET: 7 - 10 | ET-9 | ET-11 | ET-6  ET: 8 - 10 |
| **Architecture** | ARCH-15  ARCH-18 | N/A | N/A | ARCH-3 | ARCH-17  ARCH-21 |
| **Security Risk Management** | RM: 5 - 6 RM-25 RM-30 | RM: 26 - 28 RM-31 | RM-8 RM-9 | RM-4 RM-12 RM-14 RM-19 | RM: 1 - 2 RM-7  RM: 10 - 11 RM-13 RM: 15 - 16 RM-18  RM-24 RM: 32 - 34 |
| **Identity Management/**  **Privacy** | IM: 1 - 2 IM-7 | IM-3  IM: 8 – 10 | N/A | IM-5 | IM-11 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
| **Incident Management** | IR: 2 - 3 IR-20 | IR: 6 - 7 IR-11  IR: 14 - 16 IR-18 | N/A | IR-9 IR-10 IR-12 IR-14  IR-19 | IR-5 IR-8 IR-11  IR: 13 - 17 |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Securely Provision /Development

**Role Area**: Software Assurance and Software Engineering

###### Roles:

* Requirements Analyst
* Information Security Analyst
* Information Security Architect
* IA/Security Engineer
* Software Architect
* System Engineer
* Analyst Programmer
* Computer Programmer
* R&D Engineer
* Secure Software Engineer
* Reverse Engineer
* Information Owner/Steward

**Responsibility** — Develops, creates, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

###### Knowledge Unit:

* Security Risk Management
* Data Security
* Systems and Applications Security
* Architecture
* Software
* Personnel Security
* Configuration Management
* Web Security
* Modeling and Simulation
* Identity Management/Privacy
* Information Systems
* Network and Telecommunications Security

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Security Risk Management** | N/A | N/A | RM-3 RM: 7 - 8 RM-19  RM-21 | RM-22 | N/A |
| **Data Security** | N/A | N/A | DS: 3 - 10  DS: 12 - 14 DS-16  DS-18 | N/A | N/A |
| **Systems and Applications Security** | N/A | SAS-1 SAS-4 SAS-26 | SAS-1 SAS-4  SAS-6 SAS-13  SAS-21 SAS-23  SAS-26 SAS-29  SAS-31 SAS-33 | N/A | N/A |
| **Architecture** | N/A | N/A | ARCH: 1 - 2  ARCH: 5 - 17  ARCH: 19 - 21 | ARCH-1 | N/A |
| **Software** | N/A | N/A | SW: 1 - 32 | N/A | N/A |
| **Personnel Security** | N/A | N/A | PS-4  PS-11 | N/A | N/A |
| **Configuration Management** | N/A | N/A | CM: 2 - 6 CM-8 CM-11  CM: 13 - 14 | N/A | N/A |
| **Web Security** | N/A | N/A | WT-1 – 6 | N/A | N/A |
| **Modeling and Simulation** | N/A | N/A | MS: 2 - 3 | N/A | N/A |
| **Identity Management/ Privacy** | N/A | N/A | IM: 1 – 6 | N/A | N/A |
| **Information Systems** | N/A | N/A | SI: 3 - 6  SI: 9 - 11 SI-13  SI-18  SI: 20 - 22 | N/A | N/A |
| **Network and Telecommunications Security** | N/A | N/A | NTS-2 NTS-7 NTS: 9: -10  NTS: 12 - 16 | N/A | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Securely Provision/Development

**Role Area**: Systems Security and Enterprise Architecture

###### Roles:

* Enterprise Security Architect
* IA/Information Security Architect
* Principal Security Architect
* Information System Security Engineer
* Network Security Analyst
* Security Solutions Architect
* Systems Security Analyst
* Ethical Hacker

**Responsibility** — Develops system concepts and works on the capabilities phases of the systems development lifecycle translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

###### Knowledge Unit:

* Identity Management/Privacy
* Architecture
* Cryptography and Encryption
* Database
* Information Assurance
* Information Systems
* Personnel Security
* Network and Telecommunications Security
* IT Systems and Operations
* Security Risk Management
* Configuration Management
* Software
* Systems and Applications Security
* Emerging Technologies
* Modeling and Simulation

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Identity Management/ Privacy** | N/A | IM-7 | N/A | IM-1 – 5  IM: 8 – 9 | N/A |
| **Architecture** | N/A | ARCH-15 | ARCH-5 | ARCH: 5 - 6 ARCH-  9  ARCH: 11 - 12  ARCH: 14 - 17 | N/A |
| **Cryptography and Encryption** | N/A | N/A | N/A | CR-1 CR: 3 - 5  CR: 9 – 12 | N/A |
| **Database** | N/A | N/A | N/A | DB-4  DB-7 | N/A |
| **Information Assurance** | N/A | IA-2 IA-4  IA-7 | IA-8 | IA-4  IA: 6 – 7 | N/A |
| **Information Systems** | N/A | N/A | SI: 3 - 7 SI-10 SI-12 SI-16 SI-18  SI: 20 - 21  SI: 26 – 28 | SI: 1 - 3 | N/A |
| **Personnel Security** | N/A | N/A | PS-1 PS-4 | PS-11 | N/A |
| **Network and Telecommunications Security** | N/A | N/A | NTS: 7 - 9  NTS: 11 - 12  NTS: 14 – 16  NTS: 23 - 24  NTS: 30 - 31  NTS: 35 - 36 NTS-42 | NTS-16 NTS-23 | N/A |
| **IT Systems and Operations** | N/A | N/A | ITOS-4  ITOS-14 ITOS-23 | N/A | N/A |
| **Security Risk Management** | N/A | N/A | RM-4 RM: 6 - 7 RM-9  RM-26 | RM-7 RM-26 | N/A |
| **Configuration Management** | N/A | N/A | CM-5 CM-9 CM-11  CM-13 | CM-2 CM-5 CM-9  CM-11 | N/A |
| **Software** | N/A | N/A | SW: 11 - 12 | N/A | N/A |
| **Systems and Applications Security** | N/A | N/A | SAS: 1 - 2  SAS-4 SAS-6 SAS-8 SAS-11 SAS-16 SAS-  21 SAS: 22 - 23 | N/A | N/A |
| **Emerging Technologies** | N/A | N/A | ET-1 ET: 5 - 6 ET-8  ET: 10 – 11 | ET-7  ET: 9 – 10 | N/A |
| **Modeling and Simulation** | N/A | N/A | MS: 1 – 3 | N/A | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Securely Provision /Development **Role Area**: Technology Research and Development **Roles**:

* R&D Engineer
* Capabilities and Development Specialist
* Applications Security Officer
* Cloud Provider
* System Evaluator

**Responsibility** — Conducts technology assessment and integration processes provides and supports a prototype capability and evaluates its utility.

###### Knowledge Units:

* Digital Forensics
* Software
* Compliance
* Cryptography and Encryption
* IT Systems and Operations
* Information Systems
* Network and Telecommunications Security
* Architecture
* Modeling and Simulation
* Information Systems
* Physical and Environmental Security
* Procurement
* Security Risk Management
* Systems and Applications Security
* Emerging Technologies

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Digital Forensics** | N/A | N/A | N/A | DF: 3 - 4 DF-6  DF: 10 - 11  DF: 14 - 15  DF: 19 - 21  DF: 24 -25  DF: 27 - 29 | N/A |
| **Software** | N/A | N/A | SW: 2 - 3  SW: 5 - 7  SW: 11 - 12  SW: 14 - 24  SW- 30 – 32 | N/A | N/A |
| **Compliance** | N/A | N/A | N/A | COMP: 1 - 7  COMP-10 | N/A |
| **Cryptography and Encryption** | N/A | N/A | N/A | CR: 1 – 11  CR: 13 - 15 | N/A |
| **IT Systems and Operations** | N/A | N/A | N/A | ITOS: 1 – 2 ITOS-4 ITOS-7 ITOS: 9 – 11  ITOS: 13 - 15 ITOS-19  ITOS: 22 - 23 | N/A |
| **Information Systems** | N/A | N/A | N/A | SI:1 – 3  SI-5-7 SI-9-12 SI-16 SI-21 SI-26  SI-28 | N/A |
| **Network and Telecommunications Security** | N/A | N/A | N/A | NTS-7 NTS: 9 - 10 NTS-12 NTS-15 NTS-21  NTS: 23 – 24 NTS-26  NTS-30 NTS-34 NTS-36  NTS: 45 – 46 NTS-52 | N/A |
| **Architecture** | N/A | N/A | N/A | ARCH: 1 - 3  ARCH: 5 – 15 | N/A |
| **Modeling and**  **Simulation** | N/A | N/A | N/A | MS-1-3 | N/A |
| **Information Systems** | N/A | N/A | N/A | SI-5-7 SI-10  SI-21 | N/A |
| **Physical and Environmental Security** | N/A | N/A | N/A | PES-1 PES-6  PES-8 | N/A |
| **Procurement** | N/A | PROC-6  PROC: 8 - 9 | N/A | PROC: 1 - 3 | N/A |
| **Security Risk Management** | N/A | N/A | N/A | RM-3 RM: 5 - 6  RM-8 | N/A |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
| **Systems and Applications Security** | N/A | N/A | N/A | SAS: 1 – 3  SAS: 10 - 11 SAS-24 SAS-26  SAS-30 SAS-34 | N/A |
| N/A | ET: 1 - 11 | N/A |  |  |  |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Securely Provision /Development

**Role Area**: Systems Requirements Planning

###### Roles:

* Business Analyst
* Business Process Analyst
* Computer Systems Analyst
* Contracting Officer
* Contracting Officer Technical Representative (COTR)
* Human Factors Engineer
* Requirements Analyst
* Enterprise Architect
* Solutions Architect
* System Consultant
* Systems Engineer

**Responsibility** — Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

###### Knowledge Units:

* IT Systems and Operations
* Procurement
* Compliance
* Cryptography and Encryption
* Architecture
* Identity Management/Privacy
* Incident Management
* Information Assurance
* Information Systems
* Network and Telecommunications Security
* Security Risk Management
* Modeling and Simulation
* Information Systems
* Personnel Security
* Procurement
* Software
* Systems and Applications Security
* Emerging Technology

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **IT Systems and**  **Operations** | N/A | ITOS-16 | N/A | ITOS: 8 - 10 ITOS:  15 - 16 | N/A |
| **Procurement** | N/A | PROC: 1 - 12 | N/A | PROC: 1 – 5 | N/A |
| **Compliance** | N/A | COMP: 1 – 7 COMP:  9 - 10 | N/A | N/A | N/A |
| **Cryptography and Encryption** | N/A | N/A | N/A | CR: 1 – 5  CR: 14 - 15 | N/A |
| **Architecture** | N/A | ARCH 15 ARCH-18 | ARCH 1 – 21 | N/A | N/A |
| **Identify Management/**  **Privacy** | N/A | IM 1 – 3 IM-7  IM-9 | IM 1 – 3  IM -7 IM-9 | N/A | N/A |
| **Incident Management** | N/A | IR-6 | N/A | IR-10 | N/A |
| **Information**  **Assurance** | N/A | IA: 1 – 5 | N/A | IA: 6 – 8 | N/A |
| **Information Systems** | N/A | SI: 1 – 3 | SI: 1 – 7  S:I 9 – 10 SI-16  SI-18  SI: 20 – 22  SI: 24 – 26 | N/A | N/A |
| **Network and Telecommunication Security** | N/A | N/A | NTS-1 NTS-7 NTS-13 NTS-15 NTS-23  NTS-25 | N/A | N/A |
| **Architecture** | N/A | ARCH- 15 ARCH-18  ARCH-21 | ARCH 1 – 21 | ARCH 1 - 21 | N/A |
| **Security Risk Management** | N/A | RM-3  RM-6 RM-30 | RM-7 RM: 8 - 9 | RM: 2 - 3 RM-8 | N/A |
| **Modeling and Simulation** | N/A | N/A | MS 1 – 3 | N/A | N/A |
| **Information Systems** | N/A | N/A | SI: 2 - 3  SI: 12 - 13  SI: 20 - 22 | N/A | N/A |
| **Personnel Security** | N/A | N/A | PS-1  PS-4 | N/A | N/A |
| **Procurement** | N/A | PROC 1 – 12 | N/A | N/A | N/A |
| **Software** | N/A | SW-14 | SW-5 | N/A | N/A |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
| **Systems and Applications Security** | N/A | SAS-22 SAS-26 SAS-34  SAS-28 | SAS: 1 -3 SAS-26 | SAS-6 SAS-23 SAS-26 | N/A |
| **Emerging Technology** | N/A | ET: 1 – 4  ET: 8 – 11 | ET: 1- 5 | ET: 5 – 7 | N/A |

##### INFORMATION TECHNOLOGY/CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Securely Provision/Development

**Role Area**: Test and Evaluation

###### Roles:

* Application Security Tester
* Quality Assurance Tester
* Testing and Evaluation Specialist
* Systems Engineer
* R&D Engineer
* Information Systems Security Engineer
* Information Security Architect
* Ethical Hacker
* Penetration Tester
* Independent Verifiers/Validator

**Responsibility** — Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying and validating of technical, functional and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

###### Knowledge Units:

* Software
* IT Systems and Operations
* Information Assurance
* Information Systems
* Network and Telecommunications Security
* Architecture
* Information Systems
* Security Risk Management
* Identity Management/Privacy
* Systems and Applications Security

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Software** | N/A | SW-14  SW: 28 - 29 SW-32 | N/A | SW-3 SW-5 | SW-1 SW-14  SW: 22 - 23  SW: 24 - 26  SW-28 - 32 |
| **IT Systems and Operations** | N/A | ITOS- 23 ITOS-25 ITOS-27 | N/A | N/A | ITOS: 4 - 5  ITOS: 7 - 8  ITOS-10 – 15 ITOS-18 |
| **Information Assurance** | N/A | IA: 1 – 5 | N/A | N/A | IA: 1 – 9 |
| **Information Systems** | N/A | SI: 26 -28 | N/A | N/A | SI: 5 – 7  SI: 16 – 18  SI: 26 - 31 |
| **Network and Telecommunications Security** | N/A | N/A | N/A | N/A | NTS: 5 - 6  NTS: 8 - 16  NTS: 18– 40 NTS-52 |
| **Architecture** | N/A | ARCH-15 ARCH-18 | N/A | ARCH-17 | ARCH-3-5 ARCH-10 – 12  ARCH: 17 - 18 |
| **Information Systems** | N/A | N/A | N/A | N/A | SI-17  SI: 26 – 31 |
| **Security Risk**  **Management** | N/A | RM 26 – 32 | N/A | N/A | RM: 1 - 34 |
| **Identity Management/ Privacy** | N/A | IR-6 | N/A | N/A | IM-1 – 3 IR-5  IR-7 IR-10 |
| **Systems and Applications Security** | N/A | N/A | N/A | N/A | SAS 1 – 2  SAS: 9-10 SAS-12 SAS: 14 - 26 SAS-29  SAS-30 SAS-32 |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Securely Provision/Development

**Role Area**: Systems Development

###### Roles:

* IA Developer
* Program Developer
* Systems Engineer
* Information Systems Security Developer
* Information Systems Integrator
* Information Security Engineer
* IA Engineer
* Configuration Manager

**Responsibility** — Works on the development phases of the systems development lifecycle.

###### Knowledge Units:

* Software
* IT Systems and Operation
* Configuration Management
* Cryptography and Encryption
* Database
* Architecture
* Personnel Security
* Identity Management/Privacy
* Information Assurance
* Information Systems
* Network and Telecommunications Security
* Systems and Applications Security
* Security Risk Management
* Modeling and Simulation
* Procurement

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Software** | N/A | SW-14 SW-32 | SW 1 – 3  SW-5 – 11 SW-14  SW-18 – 24 SW-32 | N/A | N/A |
| **IT Systems and**  **Operations** | N/A | N/A | ITOS-4 | N/A | N/A |
| **Configuration Management** | N/A | CM-7  CM: 12 - 13 | CM: 3 - 6  CM-13 | N/A | N/A |
| **Cryptography and**  **Encryption** | N/A |  | CR-1 – 5  CR:14 - 15 | N/A | N/A |
| **Database** | N/A | DB-5 | DB-2 DB-4  DB-6 | N/A | N/A |
| **Architecture** | N/A | ARCH-15 | ARCH 9 – 14  ARCH-18 ARCH-20 | N/A | N/A |
| **Personnel Security** | N/A | PS-1  PS: 3 - 4 | PS-1  PS: 3 - 4 | N/A | N/A |
| **Identity Management/ Privacy** | N/A | IM-7 IM-9 | IM 1 – 3 IM-7 | N/A | N/A |
| **Information Assurance** | N/A | IA-1 | IA: 2 - 4  IA: 6 - 7 | N/A | N/A |
| **Information Systems** | N/A | N/A | SI: 4 – 7 SI-13  SI-16 | N/A | N/A |
| **Network and Telecommunications Security** | N/A | NTS-34 | NTS 23 – 24 NTS-26 NTS: 34 -35  NTS: 40 – 47 | N/A | N/A |
| **Systems and Applications Security** | N/A | N/A | SAS-2 SAS-20 SAS-24 SAS-26  SAS-30 | N/A | N/A |
| **Security Risk Management** | N/A | RM-26 RM-28  RM: 30 - 31 | RM-3 RM: 5 – 8 | N/A | N/A |
| **Modeling and Simulation** | N/A | N/A | MS-3 | N/A | N/A |
| **Procurement** | N/A | PROC-1 – 5 | N/A | N/A | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Securely Provision/(Assess/Evaluate) **Role Area**: Computer Network Defense Analysis **Roles**:

* CND Security Personnel
* System Administrator
* Network Security Administrator
* Network Security Specialist
* CND Analyst
* Cryptographer
* CND Auditor
* Security Analyst
* Cybersecurity Intelligence Analyst
* Focused Operations Analyst
* Incident Analyst
* Network Defense Technician
* Security Operator
* Sensor Analyst
* Information Security Architect
* Penetration Tester
* Independent Verifier/Validator

**Responsibility** — Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

###### Knowledge Units:

* Digital Forensics
* Software
* Computer Network Defense
* Configuration Management
* Compliance
* Cryptography and Encryption
* Data Security
* Incident Management/Privacy
* Information Systems
* Network and Telecommunications Security
* Architecture
* Emerging Technology
* Security Risk Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Digital Forensics** | N/A | N/A | N/A | DF 7  DF 10  DF 22 – 26 | N/A |
| **Software** | N/A | N/A | N/A | SW 4  SW 16 – 17  SW 30 – 32 | N/A |
| **Computer Network Defense** | N/A | CND 9 – 12  CND 15 – 20  CND 22 – 24 CND-29 | N/A | CND 1 - 30 | N/A |
| **Configuration**  **Management** | N/A | N/A | N/A | CM 2 - 7 | N/A |
| **Compliance** | N/A | COMP 1 – 7 | N/A | COMP 1 COMP-2 COMP 4 – 6  COMP-10 | N/A |
| **Cryptography and Encryption** | N/A | N/A | N/A | CR-12 | N/A |
| **Data Security** | N/A | N/A | N/A | DS: 11 - 12 | N/A |
| **Incident Management/ Privacy** | N/A | IM 1 – 3 | N/A | IM 1 – 5 | N/A |
| **Information Systems** | N/A | N/A | N/A | SI-15 SI-26  SI 28 – 31 | N/A |
| **Network and Telecommunications Security** | N/A | NTS – 23 NTS-52 | N/A | NTS 1 – 6  NTS-9 – 11  NTS-16 – 18  NTS 23 – 26  NTS-29 – 34  NTS 38 – 39  NTS 52 | N/A |
| **Architecture** | N/A | ARCH 15 - 16 | N/A | ARCH 7 – 9  ARCH 15 – 16 | N/A |
| **Emerging Technology** | N/A | IR 16 - 20 | N/A | IR-12 – 20 | N/A |
| **Security Risk Management** | N/A | RM 26 - 33 | N/A | RM 1 – 6 RM-10  RM-12 – 16  RM 18 – 19  RM 22 -24 RM-34 | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Assess/Evaluate

**Role Area**: Incident Response and Handling

###### Roles:

* Risk Executive
* Incident Response Personnel
* Digital Forensics Specialist
* System Administrator
* Network Administrators
* Business Contingency Planner
* IT Contingency Planner
* Damage Assessment Teams
* Information Systems Security Officer
* Computer Crime Investigator
* Incident Handler
* Incident Responder
* Intrusion Analyst
* System Evaluator

**Responsibility** — Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses planning, mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and IT/cybersecurity. Investigates and analyzes all relevant response activities.

###### Knowledge Units:

* Digital Forensics
* Computer Network Defense
* Incident Management
* Information Assurance
* Information Systems
* Network and Telecommunications Security
* Architecture
* Security Risk Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Digital Forensics** | DF-1 DF-4 | DF-6  DF: 9 - 10  DF: 23 - 26 | DF-3 DF-27 | DF-2 DF: 6 - 7 DF-9  DF-11 DF-13 DF-15  DF: 19 - 21  DF: 27 - 29 | DF-2 DF: 5 - 9  DF: 11 - 18  DF: 20 - 24  DF: 28 - 31 |
| **Computer Network Defense** | CND-1 CND-11 CND-12 CND-18 CND-20 | CND-9 CND-15 CND-29 CND-30 | CND-2 CND-17 | CND-2 CND-4 CND-6 CND-8  CND: 13 - 14  CND: 16 - 17 CND-19 CND-22  CND-28 | CND: 2 - 8 CND-10 CND-13 CND: 16 - 17 CND-19 CND: 21 - 28 |
| **Incident Management** | IR-1 IR-2 IR-20 | IR-3 IR-6 IR-11  IR: 15 - 16  IR: 18 - 19 | N/A | IR: 3 - 7 IR-10  IR: 12 - 19 | IR-3  IR: 5 - 11  IR: 13 - 15 |
| **Information Assurance** | IA-4 | IA: 1 - 2  IA-5 | IA-3  IA-6 | IA: 6 - 9 | IA-1  IA-7 |
| **Information Systems** | SI: 5 - 7 | SI: 26 - 27 SI-30 | SI-4 SI-16 SI-18 | SI-4  SI: 11 - 12  SI: 16 - 19 SI-24  SI-26  SI: 28 - 29 SI-31 | SI: 12 - 13 SI-15  SI-19 SI-23  SI: 26 - 28 SI-30 |
| **Network and Telecommunications Security** | NTS: 15 – 16  NTS: 22 - 24  NTS: 34 - 35  NTS: 42 - 43 | NTS-7 NTS-9 NTS-27 NTS-36  NTS: 38 - 39 | NTS: 12 - 14 NTS-21 NTS-26 NTS: 30 – 31 NTS-31 NTS-41 NTS-44 NTS-47 | NTS: 1 - 2  NTS: 5 - 11  NTS: 13 - 14 NTS-18 NTS: 20 – 21  NTS: 25 – 26  NTS: 28 - 33 NTS-37 NTS-39 NTS-44 NTS-52 | NTS: 3 - 6 NTS-9 NTS-11 NTS-14  NTS: 17 - 20 NTS-25 NTS: 27 – 28 NTS-33  NTS-37 NTS: 39 - 40  NTS-44 NTS-52 |
| **Architecture** | ARCH-18 | N/A | ARCH-5 ARCH-17 | ARCH-3 ARCH-7  ARCH-13 ARCH-17 | ARCH: 2 - 3 ARCH-13  ARCH-17 ARCH-21 |
| **Security Risk Management** | RM: 5 - 6 | RM: 25 - 26 RM-28 RM: 30 - 31 | RM-8 | RM-2 RM: 7 - 8 RM-10 RM-12  RM: 14 - 16 RM-19  RM: 21 - 22 | RM: 1 - 4 RM-7 RM-9  RM: 11 - 18 RM-24 RM: 32 - 34 |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Assess/Evaluate

**Role Area**: Computer Network Defense Infrastructure Support

###### Roles:

* Network Security Personnel
* Enterprise Architect
* Information Systems Security Engineer
* IDS/IPS specialist
* IDS Administrator
* IDS Engineer
* IDS Technician
* Network Security Engineer
* Security Specialist
* Information Security Architect
* System Evaluator
* Penetration Tester
* Security Control Assessor

**Responsibility** — Tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

###### Knowledge Units:

* Digital Forensics
* Computer Network Defense
* Cryptography and Encryption
* Identity Management/Privacy
* Incident Management
* Information Assurance
* Information Systems
* Network and Telecommunications Security
* Architecture
* Security Risk Management
* Web Security

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Digital Forensics** | N/A | DF 25 – 31 | N/A | DF 1 – 4 DF-6  DF 25 - 31 | N/A |
| **Computer Network Defense** | N/A | CND 1 – 30 | N/A | CND 1 - 30 | N/A |
| **Cryptography and**  **Encryption** | N/A | CR 1 - 5 | N/A | CR 1 – 8  CR 1- 15 | N/A |
| **Identity Management/ Privacy** | N/A | IM 1 – 3  IM 9 - 11 | N/A | IM 1 - 11 | N/A |
| **Incident Management** | N/A | IR 1 – 20 | N/A | IR 1 - 20 | N/A |
| **Information Assurance** | N/A | IA 1 - 9 | N/A | IA 6 - 8 | N/A |
| **Information Systems** | N/A | N/A | N/A | SI 26 - 31 | N/A |
| **Network and Telecommunications**  **Security** | N/A | NTS 21 – 26 | N/A | NTS 20 – 34  NTS 37 – 39 | N/A |
| **Architecture** | N/A | N/A | N/A | ARCH 17 – 18 | N/A |
| **Security Risk**  **Management** | N/A | RM 25 | N/A | RM 4 – 8  RM 10 - 16 | N/A |
| **Web Security** | N/A | N/A | N/A | WT 1 – 10 | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Assess/Evaluate

**Role Area**: Vulnerability Assessment and Management

###### Roles:

* Risk Executive
* Information Security Architect
* Risk/Vulnerability Analysts
* Auditors
* Ethical Hacker
* Blue Team Technician
* Close Access Technician
* CND Auditor
* Compliance Manager
* Governance Manger
* Internal Enterprise Auditor
* Penetration Tester
* Red Team Technician
* Reverse Engineer
* Risk/Vulnerability Manger

**Responsibility** — Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

###### Knowledge Units:

* Digital Forensics
* Software
* Computer Network Defense
* Procurement
* Compliance
* Personnel Security
* Identity Management/Privacy
* Information Assurance
* Information Systems
* Network and Telecommunications Security
* Architecture
* Systems and Applications Security
* Security Risk Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Digital Forensics** | N/A | N/A | N/A | DF 9 – 11 | N/A |
| **Software** | N/A | SW 28 – 30  SW- 32 | N/A | SW 22 – 27  SW-31 | N/A |
| **Computer Network Defense** | N/A | CND-29 CND 16 – 20 | N/A | CND-2 CND-4 CND-6 CND 8 – 13  CND 16 – 20  CND 22 – 30 | N/A |
| **Procurement** | N/A | PROC-3  PROC-9 | N/A | N/A | N/A |
| **Compliance** | N/A | COMP 1 – 10 | N/A | COMP 1 - 10 | N/A |
| **Personnel Security** | N/A | PS-1 – 4  PS-11 | N/A | PS-12 | N/A |
| **Identity Management/ Privacy** | N/A | IM 1- 3 | N/A | IM 1 – 5  IM 6 – 7 | N/A |
| **Information Assurance** | N/A | IA 1 – 5 | N/A | IA 1 - 7 | N/A |
| **Information Systems** | N/A | N/A | N/A | SI-16  SI 26 - 31 | N/A |
| **Network and Telecommunications Security** | N/A | NTS-39 | N/A | NTS-15 NTS 21 – 28  NTS 34 NTS-39 | N/A |
| **Architecture** | N/A | N/A | N/A | ARCH: 8 – 11  ARCH: 17 - 18 | N/A |
| **Systems and Applications Security** | N/A | SAS-2 SAS-10 SAS-12  SAS 14 – 24 | N/A | SAS-2 SAS-10 SAS-12  SAS 14 - 24 | N/A |
| **Security Risk**  **Management** | N/A | RM 1 – 34 | N/A | RM 1 - 34 | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Respond/Investigate

**Role Area**: Investigation

###### Roles:

* Incident Response Team
* Computer Crime Specialist
* Special Agent
* Special Analyst
* Information System Security Engineer

**Responsibility** — Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, analysis, interview and information gathering techniques. Processes appropriately balance the benefits of evidence gathering and safeguarding for prosecution.

###### Knowledge Units:

* + Digital Forensics
  + Compliance
  + Physical and Environmental Security
  + IT Systems and Operations
  + Security Risk Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Digital Forensics** | N/A | DF-21  DF 23 – 31 | N/A | DF 1 - 31 | DF 1 - 31 |
| **Compliance** | N/A | N/A | N/A | COMP 1 – 7  COMP 9  COMP 10 | N/A |
| **Physical and**  **Environmental Security** | N/A | N/A | N/A | PES-1  PES 4 – 6 PES-8 | N/A |
| **Security Risk Management** | N/A | RM-28 – 31 | N/A | RM 1 – 7  RM 10 – 2  RM 24 – 28  RM 32 - 34 | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Respond/Investigate

**Role Area**: Digital Forensics

###### Roles:

* Certified Computer Examiner
* Digital Forensics Analyst
* Digital Forensics Engineer
* Digital Forensics Practitioner
* Digital Forensics Professional
* CND Forensic Analyst
* Forensics Analyst (cryptologic)
* Forensics Technician
* Digital Media Collector
* Digital Forensics Examiner
* Network Forensic Examiner
* Information System Security Engineer

**Responsibility** — Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

###### Knowledge Units:

* Digital Forensics
* Software
* Computer Network Defense
* IT Systems and Operations
* Compliance
* Cryptography and Encryption
* Data Security
* Incident Management
* Information Assurance
* Information Systems
* Network and Telecommunications Security
* Architecture
* Security Risk Management
* Web Security

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Digital Forensics** | N/A | N/A | N/A | DF 1 - 31 | N/A |
| **Software** | N/A | N/A | N/A | SW 22 – 27  SW-30 | N/A |
| **Computer Network Defense** | N/A | N/A | N/A | CND 1 – 4  CND 9 – 11 CND-13  CND 16 – 21 CND-26 | N/A |
| **IT Systems and Operations** | N/A | N/A | N/A | ITOS-5  ITOS-18 ITOS-21 ITOS-26 | N/A |
| **Compliance** | N/A | N/A | N/A | COMP 1 – 7  COMP 10 | N/A |
| **Cryptography and Encryption** | N/A | N/A | N/A | CR 1 – 10  CR-14 CR-15 | N/A |
| **Data Security** | N/A | N/A | N/A | DS-2  DS-15 | N/A |
| **Incident Management** | N/A | N/A | N/A | IR 1 – 20 | N/A |
| **Information Assurance** | N/A | IA 1 – 5 | N/A | IA 1 – 5  IA-9 | N/A |
| **Information Systems** | N/A | N/A | N/A | SI 1 – 3  SI 5 – 7  SI 9 - 12 | N/A |
| **Network and Telecommunications**  **Security** | N/A | N/A | N/A | NTS 22 – 34  NTS: 37 – 41 | N/A |
| **Architecture** | N/A | N/A | N/A | ARCH 16 – 21 | N/A |
| **Security Risk**  **Management** | N/A | N/A | N/A | RM 1 – 6  RM 10 – 17 | N/A |
| **Web Security** | N/A | N/A | N/A | WT-6 | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Oversight, Management and Development

**Role Area**: Legal Advice and Advocacy

###### Roles:

* Office of General Counsel Staff
* Legal Advisor/SJA
* Cyber Lawyer
* Authorizing Executive

**Responsibility** — Provide legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and make a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

###### Knowledge Units:

* Procurement
* Compliance
* Cryptography and Encryption
* Emerging Technologies
* Security Risk Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Procurement** | N/A | PROC-6 | N/A | PROC: 6 - 9 | N/A |
| **Compliance** | N/A | N/A | N/A | COMP: 1 - 5  COMP-10 | N/A |
| **Cryptography and Encryption** | N/A | CR-1 | N/A | CR-1 | N/A |
| **Emerging**  **Technologies** | N/A | ET-1 | N/A | ET-1 | N/A |
| **Security Risk Management** | N/A | RM-30 RM-28  RM-24 | N/A | N/A | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Oversight, Management and Support **Role Area**: Strategic Planning and Policy Development **Roles**:

* Policy Analyst
* Security Policy Manager
* Policy Writer/Strategist
* IT Function Management
* IT Director
* Operations Management
* Heads of Government
* National Manager
* Program Manager
* Chief Technology Officer
* Chief Information Officer
* Command Information Officer
* IT/cybersecurity Policy Analyst
* IT/cybersecurity Policy Manager
* Risk Executive
* Mission/Business Owner

1. **Responsibility** — Applies knowledge of priorities to define an entity’s direction, determine how to allocate resources, and identify program or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

###### Knowledge Units:

* + Computer Network Defense
  + Procurement
  + Compliance
  + Architecture
  + Physical and Environmental Security
  + Information Assurance
  + Architecture
  + Security Risk Management
  + Emerging Technologies

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Computer Network Defense**  **Security** | N/A | CND-10 CND-15 CND-18  CND-29 | N/A | CND-9 CND-12 CND-15 | N/A |
| **Procurement** | N/A | PROC-1 | N/A | PROC: 1 - 5  PROC: 7 - 12 | N/A |
| **Compliance** | N/A | COMP: 3 - 5 | N/A | COMP: 1 - 7  COMP: 9 – 10 | N/A |
| **Architecture** | N/A | ARCH-15 | N/A | ARCH-5 ARCH: 15 - 16  ARCH-18 | N/A |
| **Physical and Environmental**  **Security** | N/A | PES-1 PES-6  PES-8 | N/A | N/A | N/A |
| **Information**  **Assurance** | N/A | IA 1 – 7 | N/A | IA 1 - 7 | N/A |
| **Architecture** | N/A | ARCH-15 ARCH-18 | N/A | ARCH-5 ARCH-8 ARCH-13 ARCH: 15 - 16  ARCH-18 | N/A |
| **Security Risk Management** | N/A | RM: 25 - 32 | N/A | RM: 5 - 6  RM-25 – 32 | N/A |
| **Emerging**  **Technologies** | N/A | ET: 9 - 10 | N/A | ET: 1 - 2  ET: 6 - 11 | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Oversight, Management and Support **Role Area**: Awareness, Education and Training **Roles**:

* + Security Trainers
  + End Users/System Users
  + Training Coordinators
  + Cyber Trainer
  + IT/cybersecurity Trainer
  + Human Resource Personnel

**Responsibility** — Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, and evaluates training courses, methods, and techniques as appropriate.

###### Knowledge Units:

* + IT Security Awareness and Training
  + Personnel
  + Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **IT Security Awareness**  **and Training** | SAT 1 – 12 | N/A | N/A | N/A | N/A |
| **Personnel** | N/A | PS 1 – 2 PS-5  PS-8  PS: 11-12 | N/A | N/A | N/A |
| **Management** | N/A | PM-9 PM-12  PM-53 | N/A | N/A | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Operate and Maintain

**Role Area**: Information Systems Security Operations

###### Roles:

* + Cybersecurity Officer
  + Chief Information Technology Officer
  + Enterprise Security Officer
  + Information Technology Officer
  + Senior Agency Information Technology Officer
  + Risk Executive
  + Mission/Business Owner
  + Authorizing Officials
  + Acquisition Official
  + Procurement Officer

**Responsibility** — Oversees the information assurance (IA) program of an information system in or outside the network environment may include procurement duties.

###### Knowledge Units:

* + Procurement
  + Compliance
  + Architecture
  + Incident Management
  + Information Assurance
  + Information Systems
  + Network and Telecommunications Security
  + Systems and Applications Security
  + Security Risk Management
  + Procurement
  + Identity Management/Privacy
  + Emerging Technologies

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Procurement** | N/A | PROC 1 – 12 | N/A | N/A | N/A |
| **Compliance** | N/A | COMP: 3 - 7  COMP: 9 - 10 | N/A | COMP 1 – 2  COMP-6 - 10 | N/A |
| **Architecture** | N/A | N/A | N/A | ARCH 1 – 3  ARCH 5 – 15 ARCH-18 | N/A |
| **Incident Management** | N/A | IR 1 – 3  IR 6-7  IR 11  IR 16 - 20 | N/A | IR 12 – 20 | N/A |
| **Information Assurance** | N/A | IA 1 – 5  IA-9 | N/A | IA 1 – 9 | N/A |
| **Information Systems** | N/A | SI 26 - 30 | N/A | N/A | N/A |
| **Network and Telecommunications**  **Security** | N/A | NTS 21 – 28  NTS 33- 35  NTS 38 – 39 | N/A | NTS 30 - 31 | N/A |
| **Systems and Applications Security** | N/A | SAS 10 – 12  SAS-14 – 26  SAS 28 – 34 | N/A | N/A | N/A |
| **Security Risk Management** | N/A | RM 1 - 34 | N/A | RM 1 – 34 | N/A |
| **Procurement** | N/A | PROC 7 – 12 | N/A | N/A | N/A |
| **Identity Management/ Privacy** | N/A | IM 1 – 3  IM 7 - 11 | N/A | IM 4 – 6 IM-7  IM-11 | N/A |
| **Emerging Technologies** | N/A | ET-1 ET-7  ET-9 – 11 | ET-1 | N/A | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Oversight, Management and Development

**Role Area**: Security Program Management

###### Roles:

* + 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/Risk Executive
  + CISO/SAISO
  + Common Control Provider
  + It Function Management/IT Director
  + End Users/Systems Users
  + Cloud Providers
  + Enterprise Security Officer
  + Facility Security Officer
  + Principle Security Architect
  + Senior Agency Security Officer
  + Enterprise Architect/Information Security Architect

**Responsibility:** Concentrates on protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity and availability. Manages IT/cybersecurity implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

###### Knowledge Units:

* + Digital Forensics
  + Computer Network Defense
  + Procurement
  + Compliance
  + Cryptography and Encryption
  + Incident Management
  + Information Assurance
  + Information Systems
  + Network and Telecommunications Security
  + Architecture
  + Security Risk Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Digital Forensics** | DF-4 DF-10 | DF-1 DF-6  DF 23 – 26 | DF-3 DF-6 - 7  DF-25 - 26 | DF-1 DF-3 DF-6 | N/A |
| **Computer Network Defense** | CND-15 CND 17 - 18 | CND 11 - 12 CND-29 | CND-1 CND-2 CND-4 | CND-1 CND-2 CND-4  CND-12 | CND-10 |
| **Procurement** | PROC-1 PROC-11 | PROC-2 PROC-4 PROC-6 PROC-8  PROC-12 | N/A | PROC-9 | N/A |
| **Compliance** | COMP-10 | COMP-1 COMP 3 – 5 COMP-7 | COMP-6 COMP-9 | N/A | COMP-2 COMP-5 COMP-8 |
| **Cryptography and Encryption** | N/A | CR 1 - 5 CR-10 CR-12 | N/A | N/A | N/A |
| **Incident Management** | N/A | IR 1 - 3 IR-6  IR-11 IR-16 IR-18 IR-20 | N/A | N/A | N/A |
| **Information Assurance** | N/A | IA 1 - 7 IA-9 | N/A | N/A | N/A |
| **Information Systems** | N/A | SI-26 SI-28 SI-30 | N/A | N/A | N/A |
| **Network and Telecommunications** | N/A | NTS-7 NTS-9  NTS 13 - 14  NTS 16 - 17  NTS-23 - 24 NTS-28 NTS-34 - 36  NTS-41 - 42 | N/A | N/A | N/A |
| **Architecture** | N/A | ARCH-5 ARCH 8 - 10  ARCH-12 - 15 ARCH-18 | N/A | N/A | N/A |
| **Security Risk Management** | RM-30 RM-31 | RM-3 RM-5 - 6  RM 26 - 28 | N/A | N/A | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Oversight, Management and Development

**Role Area**: Management

###### Roles:

* + Chief Information Officer (CIO)
  + Authorizing Official
  + Risk Executive
  + Senior Management
  + Senior Systems Manger
  + Program Manager
  + Project Manager
  + Functional Manager
  + Chief Information Security Officer (CISO)

**Responsibility** — Manages information programs and the security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

###### Knowledge Units:

* + Management
  + Compliance
  + Procurement
  + Identity Management/Privacy
  + Information Assurance
  + IT Security Awareness and Training
  + Personnel Security
  + Security Risk Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Management** | N/A | PM 1 - 53 | N/A | N/A | N/A |
| **Compliance** | COMP-1 COMP 4 - 5 | COMP-3 COMP-6 – 7  COMP 9 - 10 | N/A | COMP-2 COMP 9 - 10 | COMP-8 |
| **Procurement** | N/A | PROC 1 - 4  PROC 6 - 9  PROC-11 - 12 | N/A | N/A | PROC-2 |
| **Identity Management/**  **Privacy** | N/A | IM 1 - 3  IM 7 - 11 | N/A | N/A | N/A |
| **Information Assurance** | N/A | IA 1 -7  IA-9 | N/A | N/A | N/A |
| **IT Security Awareness and Training** | N/A | SAT-1 SAT-3 SAT 5 – 6  SAT 9 - 12 | N/A | N/A | N/A |
| **Personnel Security** | N/A | PS 1 - 4  PS 6  PS 8 – 12 | N/A | N/A | N/A |
| **Security Risk Management** | N/A | RM 3 - 6 RM-9  RM 18 – 20  RM 25 – 33 | N/A | N/A | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Oversight, Management and Development

**Role Area**: Privacy

###### Roles:

* + Chief Privacy Officer
  + Privacy Act Officer/Official
  + Privacy Information Professional
  + Privacy Officer
  + Senior Agency Official for Privacy
  + Human Resources
  + Health Care Officer
  + Project/Program Manager
  + Information/Business Owner

**Responsibility:** Developing and managing an organization’s privacy compliance program. Establishes 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.

###### Knowledge Units:

* + Compliance
  + Identity Management/Privacy
  + Incident Management
  + IT Security Awareness and Training
  + Management
  + Personnel Security

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Compliance** | N/A | COMP-2  COMP 4 - 7 | N/A | COMP-2  COMP 4 - 5 | COMP-8 |
| **Identity Management**  **/Privacy** | N/A | IM-1 IM-3  IM-7 IM-9 | N/A | IM 1 - 5  IM 8 - 11 | N/A |
| **Incident Management** | N/A | IR-1 IR-6 IR-16  IR-18 – 20 | N/A | IR: 15 - 16 | IR-17 |
| **IT Security**  **Awareness and Training** | N/A | SAT-1 SAT 3 - 4 | N/A | SAT 11 - 12 | N/A |
| **Management** | N/A | PM-1 – 3 PM-8  PM-11 - 13 PM-15  PM-23 PM-26 PM-34 PM-46 PM-49  PM-51 | N/A | PM-5 - 7 | N/A |
| **Personnel Security** | N/A | PS-3 PS-5 - 7  PS-1 – 12 | N/A | PS-12 | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Oversight, Management and Development

**Role Area**: Procurement

###### Roles:

* + Authorizing Official
  + Acquisition Official
  + Procurement Officer
  + Management
  + Contracting Officers
  + System Owner
  + Mission/Business Owner
  + Program Manager
  + Project Manager
  + Budgeting Officer

**Responsibility** – Procures resources as needed. Develops and executes contracts to include security controls. Ensures deliverables are compliant with Federal and Organizational security control requirements.

###### Knowledge Units:

* + Procurement
  + Management
  + Compliance

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Procurement** | PROC 1 - 2 | PROC 6 - 9 PROC-  11 - 12 | N/A | PROC-3 - 9 | PROC-4 PROC-10 |
| **Management** | PM-37 | PM-1 - 4 PM-8 PM-10 PM-12 PM-14 PM-16  PM-22 - 23 PM-25  PM-32 - 33 | N/A | PM-4 PM-6 - 8  PM-32 - 33 | N/A |
| **Compliance** |  | COMP-1 COMP-3 - 5  COMP-7 |  | COMP-2 - 5 |  |

##### INFORMATION TECHNOLOGY/CYBERSECURITY TRAINING

Module for Roles

**Function Area**: Oversight, Management and Development

**Role Area**: Personnel Security

###### Roles:

* + Hiring Manager
  + Human Resources Manager
  + First Responders

**Responsibility** – Responsible for hiring, termination and training of the IA workforce. Ensures background checks are completed. Assists with implementing the need-to-know concept. Key player in the business contingency planning and execution.

###### Knowledge Units:

* + Management
  + Personnel Security
  + Security Risk Management
  + IT Security Awareness and Training
  + Compliance
  + Identity Management/Privacy
  + Incident Management

#### Corresponding Knowledge and Skills

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Management** | N/A | PM 1 - 4  PM-6 - 8  PM-11 - 15 PM-17  PM-19 PM-23 PM-25  PM-34 - 36 PM-46  PM-48 - 51 | N/A | PM: 7 - 8 PM-11 | N/A |
| **Personnel Security** | N/A | PS-1 - 12 | N/A | PS-1 - 12 | N/A |
| **Security Risk**  **Management** | N/A | RM-25 - 31 | N/A | N/A | N/A |
| **IT Security Awareness and**  **Training** | N/A | SAT-3 SAT-6  SAT-10 | SAT-1 - 3  SAT-5 - 7 SAT-9 | SAT-4 SAT-8  SAT-1 – 12 | N/A |
| **Compliance** | N/A | COMP 1 - 7 | COMP-8 | COMP-1 | N/A |
| **Identity Management/**  **Privacy** | N/A | IM-1 - 3  IM-7 - 11 | N/A | IM-10 | N/A |
| **Incident Management** | N/A | IR-1 IR-6 IR-15 IR-20 | N/A | IR-19 | N/A |

##### INFORMATION TECHNOLOGY/ CYBERSECURITY TRAINING

Module for Roles

Function Area: Oversight, Management and Development

**Role Area**: Physical and Environmental Security

###### Roles:

* + Facility Security Officer
  + Physical Security Administrator
  + Physical Security Officer
  + First Responders
  + Physical Security Professional
  + Risk Executive

**Responsibility** – Ensures implementation and maintenance of physical security controls both in buildings hosting personnel as well as datacenters. Key player in contingency planning activities.

###### Knowledge Units:

* + Compliance
  + Enterprise Continuity
  + Incident Management
  + Industrial Controls Systems
  + Physical and Environmental Security
  + Security Risk Management

**Corresponding Knowledge and Skills**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
|  |  |  |  |  |  |
| **Compliance** | N/A | COMP-3 -5 COMP-7 COMP-  9 | N/A | N/A | COMP-8 |
| **Enterprise Continuity** | N/A | ECP: 1 - 2 ECP: 5  -6 ECP-9  ECP: 14 – 16 | ECP-3 ECP-7 - 8 | ECP: 1 -2 ECP-5  ECP: 14 - 18 | ECP: 1 - 2 ECP-4 ECP-7  ECP: 10 - 13 |
| **Incident Management** | N/A | IR: 1 - 3 IR-6  IR-12 IR-20 | N/A | IR-12 IR-14 IR-19 | IR-15 |
| **Industrial Controls**  **Systems** | N/A | ICS: 1 – 2 | N/A | ICS: 2 - 7 | N/A |
| **Physical and**  **Environmental Security** | N/A | PES-1  PES-6 PES-8 | N/A | PES: 1 - 9 | N/A |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Knowledge Unit** | **All** | **Manage** | **Design** | **Implement** | **Evaluate** |
| **Security Risk**  **Management** | N/A | RM: 25 - 28 RM:  30 – 31 | RM-8 | RM-29  RM-30 | RM-9  RM: 25 - 26 |

# Appendix D: Sample Evaluation Forms

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Evaluation Objectives** | | | | |
| **Levels of** | **Level 1:** | **Level 2:** | **Level 3:** | **Level 4:** |
| **Evaluation Student** | **Satisfaction** | **Learning** | **Performance** | **Training** |
|  |  | **Effectiveness** | **Effectiveness** | **Program** |
|  |  |  |  | **Effectiveness** |
| **Type of Training** | How well did | How did the | How well is the | Did the number |
| **CyberSecurity** | the student think | majority of | student using the | and severity of |
|  | he/she grasped | students perform | core skill set in | security |
|  | the security | on the test, (e.g., | his or her daily | incidents go |
|  | concepts? For | do aggregated | activities | down as a |
|  | CBT, how many | post-test answers | routine? | result? Did the |
|  | attempts did it | show sufficient |  | cost of security |
|  | take for the | improvement |  | compliance go |
|  | student to pass | over pre-test |  | down? If so, |
|  | the test? | answers)? |  | how much? |
| **Training** | How well did | Did the training | How well is the | Did the number |
|  | the training | program | student applying | and severity of |
|  | program fit the | demonstrably | the new security | security |
|  | student’s | and sufficiently | skills to | incidents go |
|  | expectations? | increase the | functional job | down as a |
|  |  | scope and/or | requirements? | result? Did the |
|  |  | depth of the |  | cost of security |
|  |  | student’s skill |  | compliance go |
|  |  | set? |  | down? If so, |
|  |  |  |  | how much? |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Education** | Did the course of study advance the student’s career development or professional qualifications in IT/cybersecurity  ? | Could the student apply the increased knowledge to a real world situation adequately? | How well is the student’s acquired IT/cybersecurity knowledge being used to advance agency goals & objectives? | Did the number and severity of security incidents go down as a result? Did the cost of security compliance go down? If so, how much? |

**Exhibit D-1 Evaluation Objectives**

###### Sample Questionnaire — Level 1 Evaluation Training Assessment by Student

|  |  |  |
| --- | --- | --- |
| 1. | Indicate your highest level of education: |  |
|  | High School graduate or less Some college/technical school  Associate degree or technical certification | Bachelor’s Degree Master’s Degree  Doctorate |

1. Indicate the total number of courses you have completed in subject areas related to this training:

0 1-4 5-10 11-15 More than 15

1. Indicate how long it has been since you took a course in the subject area of this training: This is my first course in this subject 4-6 years

Less than 1 year More than 6 years 1-3 years

1. Indicate the extent of your work experience in the general subject areas of this training:

|  |  |  |
| --- | --- | --- |
| None | 1-3 years | More than 6 years |
| Less than 1 year | 4-6 years |  |

1. For my preparation and level of knowledge, the training was:

|  |  |  |
| --- | --- | --- |
| Too elementary | Somewhat difficult | About right |
| Somewhat elementary | Too difficult |  |

1. The pace at which the subject matter was covered was:

|  |  |  |
| --- | --- | --- |
| Too slow | Somewhat fast | About right |
| Somewhat slow | Too fast |  |

1. For what I got out of this training, the workload was: Light

About right Heavy

1. Considering my previous experience with this subject matter, the course content was: Out of date

Somewhat current Current

1. Which of the following best describes the usefulness of this training for your job:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Not particularly useful Very useful  Somewhat useful Essential  10. How much did you learn from this training: Not much A moderate amount  A great deal  **Please send any suggestions to:** | | | | | | |
| **Student Perception of Instructor** | | | | | | |
| **Extent to which the instructor successfully:** | **Excellent** | **Good** | **Fair** | **Poor** | **N/A** | **Comments** |
| 1. Presented material in an organized manner |  |  |  |  |  |  |
| 2. Communicated knowledge of the subject matter |  |  |  |  |  |  |
| 3. Made difficult concepts understandable |  |  |  |  |  |  |
| 4. Used class time effectively |  |  |  |  |  |  |
| 5. Stimulated interest in the subject area |  |  |  |  |  |  |
| 6. Demonstrated positive attitude toward participants |  |  |  |  |  |  |
| 7. Overall, I would rate this instructor |  |  |  |  |  |  |
| **Student Perception of Course Quality** | | | | | |  |
| **Course content:** | **Excellent** | **Good** | **Fair** | **Poor** | **N/A** | **Comments** |
| 1. Clarity of course objectives |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2. Agreement between course objectives and course content |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3. Agreement between Tests/Exams and course objectives |  |  |  |  |  |  |
| 4. Degree to which the organization of the course enhanced my |  |  |  |  |  |  |
| 5. Opportunities to practice/apply course content during |  |  |  |  |  |  |
| 6. Effectiveness of textbook(s), handouts, or other material |  |  |  |  |  |  |
| 7. Quality of classroom/lab facilities |  |  |  |  |  |  |
| 8. Overall, I would rate this course |  |  |  |  |  |  |

###### Exhibit C-2 Sample Questionnaire — Level 1 Evaluation Training Assessment by Student

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sample Questionnaire — Level 3 Evaluation Training Assessment by Supervisor** | | | | | |
| **SECTION I - COURSE RELATION TO JOB REQUIREMENTS**   1. What was the chief reason for nominating the employee for this course? Information is required in present job   Information is required in new job  Course provides prerequisite or background for other training Course is required to meet certification  Course provides general career development Other (please specify)   1. Considering past experience/training and present/future job assignments, how well timed was this course in the employee’s career?   Took before needed Took when needed  Needed course earlier, but wasn’t offered Needed course earlier, but couldn’t get in  Didn’t need course and probably will never use it Unable to assess at this time   1. Which of the following best describes the usefulness of this training for the employee’s job? Essential   Very useful Somewhat useful  Not particularly useful Unable to assess at this time   1. How frequently does the employee need the skills or knowledge acquired in this course? Daily   Weekly Periodically  Not currently used, but needed for background or future use Criteria does not apply to this course  **SECTION II - COURSE IMPACT ON EMPLOYEE PERFORMANCE**  Rate the degree to which the employee’s information-related job performance was affected by the training in this course. | | | | | |
| **Job Impact** | **1** | **2** | **3** | **4** | **5** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Knowledge of IT/cyber  security- related job duties |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Technical skills (include applicable language-related skills) |  |  |  |  |  |
| Productivity |  |  |  |  |  |
| Accuracy |  |  |  |  |  |
| Use of job aids (e.g., reference aids, software applications) |  |  |  |  |  |

Overall work quality:

Legend:

1 = Greatly improved 3 = Moderately improved 5 = Not applicable

2 = First-time impact 4 = No change

###### SECTION III - RETURN ON TRAINING INVESTMENT

1. How would you describe the trade-off between the employee’s time away from the job versus IT/cybersecurity-related benefits from taking this course?

Great benefits from training offset employee time away from the job Modest benefits from training offset employee time away from the job Benefits from training did not offset employee time away from the job Do not have enough information to respond

Benefits from this course can not be measured in this manner

1. How would you respond if another employee from your area needed/wanted to take this course?

Would definitely nominate others if I knew the course was applicable to their duties Would not nominate others because Would nominate others only if the following course changes were made:

Do not have enough information to decide.

1. How knowledgeable were you about the course content before receiving this form?

I had read the catalog description or brochure and knew the expected Learning Objectives. I had read the catalog description or brochure but did not know the expected Learning Objectives.

I knew the overall purpose or goal of the course but did not read a detailed description of it and did not know the expected Learning Objectives.

I only knew the course existed.

I knew nothing about the course until I received this form.

1. As a supervisor, how satisfied are you with the training results from this course?

# Appendix E: Glossary

* + Awareness - the ability of the user to avoid behaviors that would compromise cybersecurity; practice good behaviors that will increase cybersecurity; and act wisely and cautiously, where judgment is needed, to increase cybersecurity.
  + Awareness Training - managers must ensure that all users are provided awareness training, and that those identified as having significant responsibilities for IT/cybersecurity are properly trained.
  + Base knowledge - the familiarity, awareness, or understanding of security gained through experience or study.
  + Competency – being qualified based on demonstration of an acceptable level of skills.
  + Computer Literacy - an individual’s familiarity with a basic set of knowledge with computers.
  + Cybersecurity Essentials - the transitional stage between “Basic Awareness” and “Role-based Training.” It provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.
  + Cybersecurity Learning Continuum - shows a progression of learning across the spectrum of roles within an organization.
  + Definition - provides a definition of the function.
  + Education - knowledge or skill obtained or developed by a learning process.
  + ITL – the Information Technology Laboratory (ITL) at the National Institute of Learning Objectives(s): Identifies the outcomes the training module should strive to meet for each of the functions and their associated roles.
  + Job Function - action for which a person or thing is particularly fitted or employed.
  + Knowledge Unit – the combination of information needed to perform a function or activity effectively and efficiently.
  + Literacy – an individual’s familiarity with a basic set of knowledge.
  + Proficiency *-* the state or quality of being competent
  + Role - the responsibility and functions that a person is currently performing within their agency; are established by individual Federal Organization or Agency through position descriptions, hierarchy charts, responsibilities, etc.
  + Role Areas - identifies various roles that are covered by the function. These roles are guidelines and may exist under different names within a particular Agency.
  + Security Awareness - managers must ensure that all users are provided security awareness, and that those identified as having significant responsibilities for information technology/cybersecurity are properly trained.
  + Security Literacy – an individual’s familiarity with a basic set of knowledge with security principles and practices.
  + Skills – combination of ability, knowledge, and experience that enables a person to do something well.
  + Standards and Technology - develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology.
  + Training - the action provided to a user in the acquisition of knowledge, skills, and competencies in the security arena.

# Appendix F: Acronyms

AT – Awareness and Training CBT – Computer Based Training

CISO – Chief Information Security Officer

CISSO – Computer Information Systems Security Officer CIO – Chief Information Officer

CLO – Chief Learning Officer CP – Contingency Planning DLP – Data Loss Prevention

FIPS – Federal Information Processing Standards FISMA – Federal Information Systems Management Act

FISSEA – Federal Information Systems Security Education Association IA – Information Assurance

IAM – Information Assurance Manager ICS – Industrial Control Systems

IDLS – Instructional Development Learning Systems IDP – Intrusion Detection Prevention

IDS – Intrusion Detection Systems IR – Incident Response

ISSO – Information Systems Security Officer IT – Information Technology

ITL – Information Technology Laboratory

NICCS – National Initiative for Cybersecurity Careers and Studies NICE – National Initiative for Computer Education

NIST – National Institute for Standards and Technology OJT – On-the-Job Training

OMB – Office of Management and Budget OPM – Office of Personnel Management PCI – Payment Card Industry

PII – Personal Identification Information PM – Program Manager

ROI – Return on Investment

SAISO – Senior Agency Information Security Officer SME – Subject Matter Expert

TWG – Technical Working Group VOIP – Voice Over IP

# Appendix G: References

* + FIPS 199 – entitled, “*Standards for Security Categorization of Federal Information and Information Systems,”* provides guidance on how to develop standards for categorizing information and information systems
  + FIPS 200 – entitled, “*Minimum Security Requirements for Federal. Information and Information Systems*,” introduces awareness and training as one of the seventeen areas (called “families”) of minimum security requirements identified to protect the confidentiality, integrity, and availability of Federal information systems and the information processed, stored, and transmitted by those systems.
  + NIST SP 800-100 – entitled, “*Information Security Handbook: A Guide for Managers*” describes how to manage information security in your organization.
  + NIST SP 800-37 – entitled, “*Guide for Applying the Risk Management Framework to Federal Information Systems,”* addresses the risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, instructions, standards, Instructions, or regulations.
  + NIST SP 800-50 – entitled, “*Building an Information Technology Security Awareness and Training Program,”* describes the following key approaches of an IT/cybersecurity awareness and training program that “Federal Organizations” (i.e., Federal agency/departments, Agencies or organizations) should follow.
  + NIST SP 800-53 – entitled, *“Security and Privacy Controls for Federal Information Systems and Organizations,”* provides more detail to the awareness and training area identified in FIPS 200 and provides levels for each control, dependent upon the system categorization and corresponding baseline.
  + NIST SP 800-53A – entitled, *“Guide for Assessing the Security Controls in Federal Information Systems,”* provides guidelines for the assessment of the effectiveness of implemented awareness and training controls within an organization.
  + NIST SP 800-160 – entitled, “*Systems Security Engineering,”* provides a definition and discussion of Systems Security Engineering as an engineering discipline.
  + The National Initiative for Cybersecurity Education (NICE) - developed the National Cybersecurity Workforce Framework (“the Framework”) to provide a

common understanding of and lexicon for cybersecurity work.