Withdrawn Draft

Superseding Document

Status	2nd Public Draft (2PD)
Series/Number	NIST Special Publication 800-16 Revision 1
Title	A Role-Based Model for Federal Information Technology/Cybersecurity Training
Publication Date	October 2013
DOI	
CSRC URL	https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/archive/2013-10-24
Additional Information	

Information Security Training Requirements: A Role- and Performance-Based Model (Draft)

Recommendations of the National Institute of Standards and Technology

Mark Wilson
Kevin Stine
Pauline Bowen

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March, 2009

Reports on Information Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology 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 nonnational-security-related information in federal information systems. This 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.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, and for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security 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 A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright regulations. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict 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.

Acknowledgements

Notes to Reviewers

There are several things that we ask that you focus on as you review this draft publication. They are:

- <u>Audience</u>: This publication is unlike many NIST Special Publications (SPs) because it is primarily intended to be read and understood by two rather diverse populations, information security professionals and instructional design specialists (IDSs) (or training development specialists). We believe that these two audiences will look at the document in very different ways. The information security professional will probably be reading to understand what must be done to provide role-based training in his or her organization. The instructional design specialist/training development specialist will be reading to understand the training methodology contained in the document, and to use that methodology to design and possibly present training courses for specific audiences. We would like to know if this document is understood by these two populations of people.

- <u>Intended audience icons or tags</u>: We decided to employ icons or tags to mark chapters and sections to identify which audience, information security or training development, should focus on that chapter and/or section. Does it help to use these icons? Are they applied in a helpful manner?

- <u>Awareness Training: Basics and Literacy</u>: In our guidelines to date, we have used the terms "awareness" and "training." When FISMA introduced the term "awareness training" we equated that to awareness. This is reflected throughout SP 800-50 and in SP 800-100. However, the Information System Security Line of Business (ISS LOB) Tier 1 Awareness Training initiative has focused on the need for training-like material for users of information and information systems. This is the audience that the original authors of SP 800-16 had in mind when they developed the Basics and Literacy chapter and the Basics and Literacy level of the Learning Continuum. The ISS LOB Tier 1 Awareness Training Shared Service Centers (SSCs), the federal departments or agencies selected to provide awareness training material to other federal customers, are expected to provide web-based, computer-based, or in-person-delivered awareness training material. In this draft, we are equating awareness training with basics and literacy, and the intended audience is all users of information and information systems. This still leaves the Awareness level of the Learning Continuum intact; the target audience of awareness efforts is all employees. Typical traditional awareness initiatives will still include use of posters, trinkets, post-it notes, e-mail advisories, computer security (or information security) day events, etc. The Role-Based Training and Education levels of the Learning Continuum are also unaffected by this change. We have discussed this proposed change with the Federal Information Systems Security Educators' Association (FISSEA) Executive Board, and presented it at annual FISSEA Conferences and periodic free FISSEA workshops, and at the Federal Computer Security Program Managers' Forum offsite. To date, this change has been welcomed. Will this work for you and your organization?

- <u>Additional topic details</u>: In this draft document, we have attempted to provide another level of detail that should help instructional design specialists build training courses and modules. We have added this material to the Information Security Training Topics and Elements that are introduced in Exhibit 4-4 and used throughout Appendix B to identify the material that should be considered for inclusion in each module (or cell) used in each training course or module. Does this help? If not, what enhancement would you recommend we consider?

- Discussion on significant responsibilities for information security: In our planned update of SP 800-50 (scheduled to begin this fiscal year) we expect to significantly expand the discussion of identifying those personnel who have significant responsibilities for information security, the key role-based training passage in FISMA. Because we plan to cover that topic in the update of SP 800-50, we have not done so in this document. We decided that SP 800-50, the information security awareness and training program-level guideline, is the proper document for that in-depth discussion, and that SP 800-16, Rev. 1 should continue to focus on the role-based training methodology. We believe that by the time someone opens SP 800-16, Rev. 1, the department or agency should have already decided who in the organization has significant responsibility for information security, and that SP 800-16, Rev. 1 would then be used to develop information security training courses or modules for those people. Do you agree with this approach?

- A "catalog" of roles: In Exhibit 4-1 and in Appendix A, we list roles that have some information security responsibilities in some or most organizations. We emphasize that this list of roles should be viewed as a catalog of roles, and not the answer to the question, "Who has significant responsibility for information security?" We use the notion of "catalog" to suggest that once an organization determines who has significant responsibility for information security, the information security program staff and/or instructional design specialist then refer to this document to find the role previously identified and begin to develop a course or module. Does this use of "catalog" work for you and your organization? Does it emphasize enough the "select what you need" approach, as opposed to the "the role is listed in SP 800-16, so we must build a course for it" approach that some have taken?

- Use of Job Task Analysis and Role Matrices as "Starting Points": In Chapter 4 we emphasize the need for a job task analysis to identify what information security training is needed for a specific role or group of people in an organization. We also state that the cells that are identified for each role-based matrix in Appendix A should be considered to be starting points, that the mix of cells per role will probably vary from one organization to another, and that a job task analysis – or policy review, subject matter expert review, or some other type of review – will determine more precisely what cells – what information – should be included in a training course or module. We have done this to move further away from the "one size fits all" view that some have read into the current publication's use and description of the role-based matrices. Does this additional flexibility help you and your organization?

- Proliferation of Information Security Training and Workforce Development "Standards" or "Guidelines": NIST SP 800-16 is now one of at least five or six information security (or cyber security) training and workforce development initiatives that are either under development or completed. The other initiatives include the training standards developed by the Committee on National Security Systems (CNSS), the Essential Body of Knowledge (EBK) developed by the Department of Homeland Security (DHS), the 2210 Series competencies and training topics developed by the Office of Personnel Management (OPM), the Information Security Workforce Development Matrix Project being developed by the CIO Council's IT Workforce Committee, and the "cyber education" (including training) initiative being developed as part of the Cyber Initiative. In addition to these standards and guidelines, there are several noteworthy community-wide efforts including the Department of Defense's 8570 information assurance training and certification program and the Office of the Director of National Intelligence (ODNI) Cyber Training Subdirectory. These efforts are serving, or are being developed to serve, large communities within the federal sector, and also deserve recognition and

consideration along with the aforementioned initiatives. During the writing of this update to SP 800-16, NIST began to reach out to the owners or stakeholders of these other initiatives. We are seeking to: 1) better understand the purpose and intended audience(s) of each of the initiatives, and 2) begin a harmonization effort between all of the initiatives, with the goal being to determine how they relate to each other, and if needed and agreed upon by initiative owners or stakeholders, how changes can be made that result in a homogeneous set of standards, without duplication of effort or confusion among the initiatives' constituents or communities. One possible outcome of this harmonization effort that we envision is that NIST SP 800-16, Rev. 1 might serve as a fairly general foundational document, from which the other training and workforce development initiative publications and community-wide programs could be seen as tailor-fit efforts for their particular communities. These communities would or could include National Security, Defense, Intelligence, Law Enforcement, and Homeland Security. In order for this possible model to work, NIST SP 800-16, Rev. 1 would have to be general enough as to not conflict with any community-specific work. Although this harmonization effort is not part of this document, we welcome your thoughts about the existing and under-development initiatives, and about a harmonization effort that will result in a "wiring diagram" that explains the relationship between the initiatives, and/or a foundational document that supports community-specific efforts. As you review this draft document, please consider if it is general enough to dovetail with community-specific training and workforce development initiatives while still being specific enough to be useful to help meet your role-based training needs, or is it too specific, or too general? What do you think the role of SP 800-16, Rev. 1 should be, relative to these other initiatives?

Table of Contents

Executive Summary

This publication updates a document that was first published in April 1998. Since the initial publication date, there has been an increase at the national level in the attention paid to, and the need for, a properly trained information security workforce. The Federal Information Security Management Act (FISMA) of 2002 not only requires organizations to ensure that all users of information and information systems are aware of their information security responsibilities, but also requires departments and agencies to identify and train those with "significant responsibilities for information security." Though FISMA does not specify role-based training for these individuals, the Office of Personnel Management (OPM) does in their June 2004 mandate – 5 CFR, Part 930. The OPM regulation reinforces what FISMA states regarding users being exposed to information security awareness, or "awareness training." OPM takes the FISMA requirement for training of those with significant responsibilities for information security a step further, specifying "role-specific training in accordance with NIST standards and guidance." This publication updates what was presented in 1998, and captures these latest federal mandates regarding information security "awareness training" and "role-based training."

In Special Publications to date, NIST has described and discussed "awareness" and "training" when documenting federally mandated learning which various audiences must receive. FISMA introduced the term "awareness training." NIST publications since FISMA have equated "awareness training" with "awareness." However, the Information Systems Security Line of Business (ISS LOB) Program identified awareness training as a LOB. The subsequent direction provided by the Office of Management and Budget (OMB) to the Shared Service Centers (SSCs) – those government organizations selected to provide information security awareness training to the federal government – suggested that the material developed by the SSCs be more akin to formal (e.g., web-based, computer-based, in-person delivered) training than to typical awareness efforts (e.g., security slogans, trinkets, posters, pens, post-it notes). This gave awareness training a different look than traditional awareness – a look more like training material for users of information and information systems. It is for this reason that this publication describes and differentiates "awareness," "awareness training" and "(role-based) training" for the first time. The Learning Continuum – described in Chapter 2 of this document – re-labels "Security Basics and Literacy" (as originally used in the 1998 publication) as "Awareness Training: Basics and Literacy." It is learning directed at users of information and information systems. Functionally, there is no difference between the Basics and Literacy level of the Learning Continuum in the original publication and this new approach or label. "Awareness training" is very much information security basics and literacy for users of information and information systems.

This publication is unlike many NIST Special Publications because it is primarily intended to be read and understood by two rather diverse populations – information security professionals and instructional design specialists/training development specialists. We believe that these two audiences will look at the document in very different ways. The information security professional will probably be reading to understand what must be done to provide role-based training in his or her organization. The instructional design specialist/training development specialist will be reading to understand the training methodology contained in the document, and to use that methodology to design and possibly present training courses for specific audiences.

Because this document has been written to be understood, for the most part, by these two diverse audiences, we decided to employ icons or tags to mark chapters and sections to identify which audience should focus on that chapter and/or section. This is one change among many that we have made in this version of the publication, hoping that it improves the document in the eyes of our constituency.

In this document, we have attempted to provide another level of detail that should help instructional design specialists build training courses. We have added this material to the Information Security Training Topics and Elements that are introduced in Exhibit 4-4 and used throughout Appendix B to identify the material that should be developed for each cell or module that is used in each training course.

Chapter 1

1. Introduction

Federal departments and agencies are clearly tasked to protect information entrusted to the federal government by the American public. Federal laws and supporting policies, requirements, standards, and guidelines task numerous individuals throughout an organization – from agency heads to users, and many people in between – with a variety of responsibilities. These responsibilities include identifying information 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 controls, authorizing the use of the systems, and maintaining an effective information security posture by being vigilant and carrying out their specific security-related responsibilities.

Meeting these responsibilities and providing for the confidentiality, integrity, and availability of information in today's highly networked environment is not an easy or trivial task. The task is made that much more difficult, if not impossible, if each person who owns, uses, relies on, or manages information and information systems does not know their specific responsibilities and/or is not properly motivated to carry out their information security responsibilities.

This document and NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program* describe the following key approaches of an information security awareness and training program that federal departments and agencies should follow to help ensure that individuals learn the appropriate information security-related material:

- All employees of an organization must be regularly or continually exposed to *information security awareness* techniques (e.g., posters, awareness tools/trinkets, periodic e-mail, warning messages, tips of the day upon accessing an information system, computer/information security day events).

- All users of information and information systems must attend *information security awareness training* (on-line or in-person) each year. This material should provide the information security basics and literacy as described in Chapter 3 of this document. This basics and literacy knowledge serves as the foundation upon which role-based training is built for those with significant responsibility for information security.

- Each person who has been identified by his or her organization as having significant responsibility for information security must receive formal *role-based information security training*.[1] The amount and frequency of training depends on the gap between an individual's existing and needed skills, and changes in technology and the operating environment to which the individual must adapt. Influences on training needs include individual development plans (IDPs), performance plans, and management.

1.1. Legislative and Policy Drivers

The Federal Information Security Management Act (FISMA), signed into law in 2002, fine-tuned long-standing information security awareness and training requirements. FISMA clearly distinguishes between awareness efforts and training.

---

[1] While the phrase "role-based training" is used extensively in this document to describe that training to be provided to people who have significant responsibility for information security, 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 "awareness training," which provides information security basics and literacy, the foundation of information security knowledge for users, upon which the additional role-based training is built.

- 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 Chief Information Officer (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 then ensure that they are trained to the level needed to perform their security-related tasks.

In June 2004, the Office of Personnel Management (OPM) issued a revision to the federal personnel regulations. The changes build upon information security awareness and training requirements contained in FISMA, and capture key concepts from NIST Special Publications 800-50 and 800-16. This regulation, 5 CFR Part 930, is entitled "*Information Security Responsibilities for Employees Who Manage or Use Information Systems*" and requires federal agencies to provide training as set forth in NIST guidelines. Key requirements from the OPM regulation include:

- develop an information security awareness and training plan;

- identify employees with significant information security responsibilities and provide role-specific training in accordance with NIST standards and guidelines;

- expose all users of federal information systems to information security awareness materials at least annually;

- provide the following groups training that includes specific material;

  – executives,

  – program and functional managers,

  – CIOs, information security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers),

  – IT function management and operations personnel;

- provide information security awareness and training to all new employees before allowing them access to systems;

- provide information security 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.

Office of Management and Budget (OMB) Circular A-130, "*Management of Federal Information Resources,*" Appendix III, "*Security of Federal Automated Information Resources,*" although the oldest of the three key federal information security mandates cited in this section, 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.

1.2. Relationships with Other NIST Documents

In October 2003, NIST published Special Publication 800-50, *"Building an Information Technology Security Awareness and Training Program."* SP 800-50 was designed to be a companion document to SP 800-16, serving as a foundation document for federal organizations that needed to build or fine-tune an information security awareness and/or training program. SP 800-50 points to SP 800-16 in that section that discusses the development of information security training material. The two publications are complimentary – SP 800-50 works at a higher strategic level, discussing how to build an information security awareness and training program, while SP 800-16, Rev. 1 is at a lower tactical level, describing an approach to information security awareness training and role-based training.

FIPS 200, *"Minimum Security Requirements for Federal Information and Information Systems,"* introduces awareness and training as one of the seventeen areas (later 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 Special Publication 800-53, *"Recommended Security Controls for Federal Information Systems,"* provides more detail to the awareness and training area identified in FIPS 200 by documenting five specific controls in the Awareness and Training (AT) control family.[2]

NIST Special Publication 800-53A, *"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.

1.3. Purpose and Scope

This document is intended to be used by federal information security professionals and instructional design specialists to accomplish two major tasks; 1) design role-based training courses or modules for department or agency personnel who have been identified as having significant responsibilities for information security, and 2) design a *basics and literacy* course for all users of information systems.[3] The basics and literacy course is intended to meet the FISMA requirement for *awareness training*[4] and should be not be confused with the lowest level of learning discussed in this document – *awareness.*[5]

This document describes information security awareness, awareness training, role-based training, education, and certification. However, its primary focus is providing a comprehensive training methodology for the development of training courses or modules for a number of roles of personnel who have been identified as having significant information security responsibilities within departments and agencies.[6] This document's secondary focus is providing a curriculum for a basics and literacy – awareness and training – course for all users.[7]

---

[2] SP 800-53, Rev. 2 and Rev. 1 identified five AT controls. The original SP 800-53 document identified four AT controls.

[3] Those personnel identified as having significant responsibility for information security should receive awareness training as the foundational basics and literacy for users, **and** role-based training to address their additional responsibilities for having been identified as having significant responsibility.

[4] The basics and literacy section is also designed to meet the needs of the Shared Service Centers (SCCs) that are providing information security awareness training material to federal organizations under the Information Systems Security Line of Business (ISS LOB) Tier I – Awareness Training – Program, managed and implemented by OMB and the Department of Homeland Security (DHS).

[5] Awareness, awareness training, and role-based training are discussed in greater detail in Chapter 2.

[6] Although this document includes a number of role-based matrices in Appendix B, by no means does this suggest that any organization should have to build training courses or modules for each role. Appendix B should be viewed as a catalog of role-specific matrices, some of which will be used to build courses or modules. Organizations should have

1.4. Audience

This document was written primarily for two audiences: the information security professional that has responsibility for designing and implementing the security awareness training and role-based training portions of an organization's information security awareness and training program, and the instructional design specialist who is tasked with developing and possibly delivering the awareness training and role-based training material and courses (or modules).

The information security professional and the instructional design specialist will have different motivations and different needs when reading this document.

Since this document is written for these two different primary audiences, and in an attempt to guide these audiences through the document, icons have been placed in the chapter [and section?] headings, indicating for which primary audience the chapter [and section?] was written. The icon for the information security professional is [security icon here] while the icon for the instructional design specialist is [trainer icon here].

In addition to the two primary audiences for whom this document was written, this publication should also be read, reviewed, or understood at a fairly high level by several other audiences.

- The senior agency information security officer (SAISO)[8], other information security program managers and staff, and auditors should be familiar with the scope of this document, and should understand the applicability of the basics and literacy course (awareness training) and of the role-based courses or modules for those who have been identified as having significant responsibilities for information security.

- The organization's CIO should understand that this document contains topics and a curriculum that can be used to develop a basics and literacy course to meet the FISMA awareness training requirement, and a thorough training methodology that can be used to develop role-based training courses or modules[9] for those people who have significant responsibilities for information security.

1.5. Roles and Responsibilities

While it is important to understand the policies that require departments and agencies to develop information security awareness training courses and specialized or role-based training courses or modules, it is crucial that organizations understand who has responsibility for identifying the target audiences and developing the awareness training and role-based training material.

1.5.1. Agency Head

Agency heads must ensure that high priority is given to effective information security awareness, awareness training, and role-based training for the workforce. This includes implementation of a

---

identified those personnel or roles needing role-based training, based on their having significant responsibility for information security, before using this document.

[7] The subject of developing information security awareness material is discussed in NIST SP 800-50. Information security education and certification are not within the scope of this document (or other NIST publications) because there is no federal government-wide policy that requires information security education or certification.

[8] While FISMA introduces the term SAISO, some departments and agencies still use "IT Security Program Manager," "Chief Information Security Officer," "Chief Information Assurance Officer," "Information Assurance Officer," or other terms to denote the person responsible for the organization's information security program.

[9] Information security training modules are best developed and deployed in situations where functional training is developed and provided, but without adequate coverage of those issues necessary for the individual to perform their information security responsibilities. A security module can be added to existing functional training, or provided separately, if integrating the security module into the functional training course is not feasible.

viable information security program with a strong awareness and training component. Agency heads should:

- Designate a CIO;
- Assign responsibility for information security;
- Ensure that an agency-wide information security program is implemented, is well-supported by resources and budget, and is effective; and
- Ensure that the agency has enough sufficiently trained personnel to protect its information resources.

1.5.2. Chief Information Officer

Chief Information Officers (CIOs) are tasked by the FISMA to administer training and oversee personnel with significant responsibilities for information security. CIOs should work with the SAISO to:

- Establish overall strategy for the information security awareness and training program;
- Ensure that the agency head, senior managers, system and information owners, and others understand the concepts and strategy of the information security awareness and training program, and are informed of the progress of the program's implementation;
- Ensure that the agency's information security awareness and training program is funded;
- Ensure the training of agency personnel with significant responsibilities for information security;
- Ensure that all users of information systems are sufficiently trained in their security responsibilities and other information security basics and literacy through awareness training;
- Ensure that an effective information security awareness effort is developed and employed such that all personnel are routinely or continuously exposed to awareness messages through posters, e-mail messages, logon banners, and other techniques; and
- Ensure that effective tracking and reporting mechanisms are in place.[10]

1.5.3. Senior Agency Information Security Officer

The SAISO has tactical-level responsibility for the organization's information security awareness and training program. In this role, the SAISO should:

- Ensure that awareness, awareness training, and role-based training material developed or purchased is appropriate and timely for the intended audiences;
- Ensure that awareness, awareness training, and role-based training material is effectively deployed to reach the intended audiences;
- Ensure that employees, users, those receiving role-based training, and managers have an effective way to provide feedback on the awareness, awareness training, and role-based training material and its presentation;
- Ensure that awareness, awareness training, and role-based training material is reviewed periodically and updated when necessary; and

---

[10] While attendance in awareness training and role-based training courses and classes can be tracked and reported, exposure to information security awareness techniques is difficult to quantify and equally difficult, if not impossible, to track and report.

- Assist in establishing a tracking and reporting strategy.

1.5.4. Managers

Managers have responsibility for complying with information security awareness, awareness training, and role-based training requirements established for their employees, users, and those who have been identified as having significant responsibilities for information security. Managers should:

- Work with the CIO and SAISO to meet shared responsibilities;

- Serve in the role of system owner and/or information owner, where applicable;[11]

- Consider developing individual development plans (IDPs) for those with significant security responsibilities;

- Promote the professional development and certification of the information security program staff, full-time or part-time information security officers, and others with significant responsibilities for information security;

- Ensure that all users (including contractors) of their systems (i.e., general support systems and major applications) are appropriately trained in how to fulfill their information security responsibilities before allowing them access;

- Ensure that users (including contractors) understand specific rules of each system and application they use; and

- Work to reduce errors and omissions by users due to lack of awareness, awareness training, and/or specialized role-based training.

1.5.5. Instructional Design Specialists

Instructional design specialists (IDSs), whether internal to an organization or external, are key players in an information security awareness and training program. An organization usually requires the assistance of IDSs for the development of awareness, awareness training, and role-based courses. IDSs should:

- Work with an information security subject matter expert when developing awareness, awareness training, and/or 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;

- Understand the basics and literacy section of this publication since it is used to develop awareness training courses for users of information systems; and

- Understand the role-based training methodology in this document since it is used to develop specialized courses or modules for those individuals who have been identified as having significant responsibilities for information security.

1.5.6. Personnel with Significant Responsibilities for Information Security

FISMA requires agencies to identify and train those personnel with significant responsibilities for information security. These personnel - whether executives, information security 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

---

[11] Managers who serve as owners of general support systems and major applications have responsibility for the overall information security of those systems and applications, including ensuring that all users are exposed to awareness and awareness training, and that those who are identified as having significant responsibilities for information security are trained.

have the greatest positive or negative impact on the confidentiality, integrity, and/or availability of agency information and information systems. Specialized role-based information security training is necessary to help ensure that these "keys to security" clearly understand that information security is an integral part of their job; what the organization expects of them; how to implement and maintain information security controls; mitigate risk to information and information systems; monitor the security condition of the security program, system, application, or information for which they are responsible; and/or what to do when security breaches are discovered. 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, and

- Apply what is learned during training.

1.5.7. Users

Users are the largest audience in any organization and 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 agency personnel, visitors, guests, and other collaborators or associates requiring access to information and/or systems. Users must:

- Understand and comply with agency information security policies and procedures;

- Be appropriately trained in the rules of behavior for the systems and applications to which they have access;[12]

- Work with their management to meet awareness and/or awareness training needs;

- Keep software/applications updated with security patches in those cases in which users are responsible for doing so; and

- Be aware of actions they can take to better protect their organization's information. These actions include, but are not limited to, proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of information security policy, and following rules established to avoid social engineering attacks and rules to deter the spread of spam or viruses and worms.[13]

1.6.   Who Should Use the Document

CIOs and other executives should refer to this document to gain a basic understanding, beyond what is mentioned in NIST SP 800-50, of their organization's responsibilities regarding information security awareness, awareness training, and role-based training. SAISOs and other information security practitioners should use this document to become familiar with the requirements for information security awareness training and role-based training, and to determine at which point they hand over responsibility for material development to instructional design specialists. Instructional design specialists should use this document to identify the topics that should be included in information security awareness training courses, and to use the role-based training methodology to build specialized training courses.

---

[12] All employees must be exposed to information security awareness material. All users of information systems must receive awareness training.

[13] These are typical examples of messages portrayed in security awareness posters, tools/trinkets, tips of the day, etc. However, these topics can be expanded upon and combined with information security basics and literacy material identified in Chapter 3 and developed into an awareness training course for all users of information systems.

1.7. Document Organization

This guideline is divided into four chapters and four appendices.

- Chapter 1 (this chapter) describes the legislative and policy drivers, relationships with other NIST documents, purpose and scope, audience, roles and responsibilities, and outlines the organization of this document.

- Chapter 2 describes the learning continuum (e.g., information security awareness, awareness training, specialized role-based training, and education), and the model of the continuum.

- Chapter 3 describes the information security basics and literacy level of the model – the curriculum that makes up the awareness training course for users of information systems.

- Chapter 4 describes the implementation of role-based training, utilization of role-based training matrices and curriculum modules, and contains a step by step description of the process of building a role-based training course or module.

- Appendix A contains the role-based matrices.

- Appendix B contains the information security training curriculum modules.

- Appendix C contains recommendations for evaluating training effectiveness.

Chapter 2

2. Learning Continuum – Model and Overview

2.1. Introduction to the Model

The model presented as Figure 2-1 is based on the premise that learning is a continuum. 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.

The model is role-based. It defines the information security learning needed as a person assumes different roles within an organization and different responsibilities in relation to information systems. This document uses the model to identify the knowledge, skills, and abilities an individual needs to perform the information security responsibilities specific to each of his or her roles in the organization.

The type of learning that individuals need becomes more comprehensive and detailed at the top of the continuum. Thus, beginning at the bottom, all employees need to be exposed to awareness. All information system users need awareness training. Special training is required for individuals whose role in the organization indicates a need for special knowledge of information security threats, vulnerabilities, and safeguards. The "Education" layer of the model applies primarily to individuals who have made information security their profession.

The model illustrates the following concepts:

- "Basic Security Awareness" is explicitly required for employees, including contractor employees who are involved in any way with information systems. In today's environment this typically means all individuals within the organization.

- "Awareness Training (Basics and Literacy)," is a 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, skills, and abilities specific to an individual's roles and responsibilities relative to information systems. At this level, training recognizes the differences between beginning, intermediate, and advanced skill requirements.

- The "Education" level focuses on developing the ability and vision to perform complex multi-disciplinary activities and the skills needed to further the information security profession and to keep pace with threats and technology changes.

- The "Professional Development" is intended to ensure that users, from beginner to the career security professional, possess a required level of knowledge and competence necessary for their roles. Professional development validates skills through certification and advanced education such undergraduate and graduate studies and degrees.
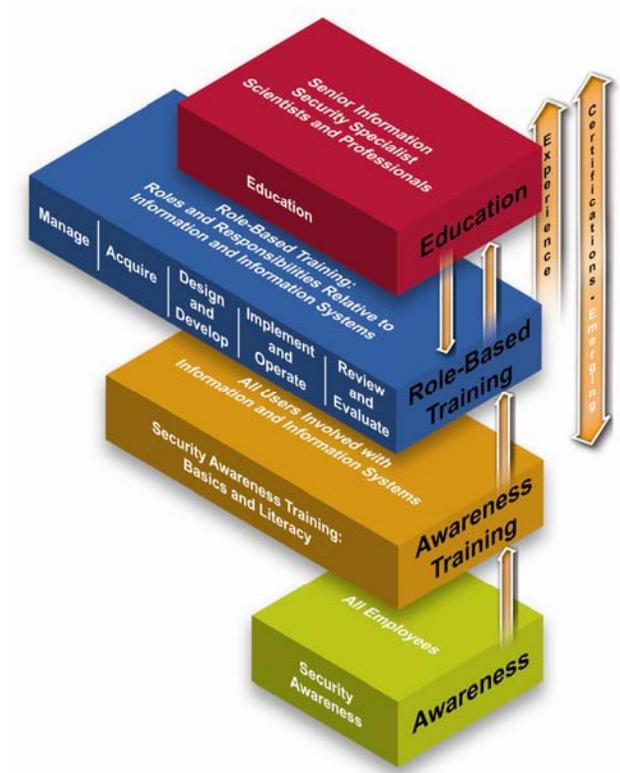
Figure 2-1: Information Security Learning Continuum

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 information security 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.

2.2. Levels of Learning

2.2.1. Awareness

Awareness is not training. 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 an issue or a set of issues. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize information security concerns and respond accordingly.

In awareness activities the learner is a 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 job performance.

A few examples of information security awareness materials/activities include:

- Events, such as an information security day,

- Briefings (program- or system-specific or issue-specific)

- Promotional/specialty trinkets with motivational slogans,

- A security reminder banner on computer screens, which comes up when a user logs on,

- Security awareness video tapes, and

- Posters or flyers.

Effective information security awareness efforts must be designed with the recognition that people tend to practice a tuning-out process called acclimation. If a stimulus, originally an attention-getter, is used repeatedly, the learner will selectively ignore the stimulus. Thus, awareness delivery must be on-going, creative, and motivational, with the objective of focusing the learner's attention so that the learning will be incorporated into conscious decision-making. This is called assimilation, a process whereby an individual incorporates new experiences into an existing behavior pattern.

Learning achieved through a single awareness activity tends to be short-term, immediate, and 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.

The fundamental value of information security awareness programs is that they set the stage for awareness training and role-based training by bringing about a change in attitudes which should begin to change the organizational culture. The cultural change sought is the realization that information security is critical because a security failure has potentially adverse consequences for everyone. *Therefore, information security is everyone's job.* Detailed guidance on information security awareness is outside the scope of this document, but is covered in more depth in NIST SP 800-50.

2.2.2 Awareness Training (Basics and Literacy)

The Awareness Training: Basics and Literacy level of the learning model is the bridge between awareness and role-based training. Awareness training strives to build in an organization's information system user population a foundation of information security terms and concepts upon which later role-based training, if required, can be based. Awareness training 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. Awareness training not only communicates information security policies and procedures that need to be followed, but also provides the foundation for any sanctions and disciplinary actions imposed for noncompliance. Awareness training is used to explain the rules of behavior for using a department's or agency's information systems and information and establishes a level of expectation on the acceptable use of the information and information systems. Awareness training is covered in depth in Chapter 3.

2.2.3 Role-Based Training

Information security 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 information security. Training supports competency development and helps personnel understand and learn how to better perform their security role. The most important difference between training and awareness is that training seeks to teach skills that allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or a set of issues.

The role-based training methodology contained in this document begins in Chapter 4.

2.2.4 Education

The Education level of the Learning Continuum represents the additional option that both current and prospective information security professionals have to build or enhance their security-oriented knowledge and skills. The increasing number of students going through degree and certificate programs at colleges and universities also gives management an additional avenue by which to bring information security professionals into the workforce, beyond the traditional "train them when you get them" approach.

2.2.5 Professional Development

Information security professionalization is rapidly becoming a "business competency" in the public and private sectors.

At the advanced level of information security professionalization, such as that of an Information Security Program Manager, an employee should be able to represent the organization and participate actively and constructively in addressing interagency or cross-cutting issues and concerns. Examples include increasing the effectiveness of security techniques and controls; developing security policy models; participating in symposia or workgroups; or contributing to, developing, or managing information security training programs.

To reach the advanced level of information security 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 information security field can be seen among information security officers, information security auditors, information technology contractors, and system/network administrators, and is evolving. An example of education that leads to professionalization is a degree program at a college or university at the undergraduate, graduate or doctorate level.

The training methodology that is described in Chapter 4 can be used and sequenced by organizations on an individualized basis as a cost-effective way to fill gaps in a given practitioner's knowledge and prepare him/her for formal education that may be needed for credentialing or other demonstrable measures of qualification in the information security profession.

Chapter 3

3. Awareness Training: Basics and Literacy

3.1. Definition and Purpose

The *Information Security Awareness Training: Basics and Literacy* level on the learning continuum is the transition between awareness and role-based training. To draw an analogy with reading literacy, "awareness" is equivalent to reading readiness, whereby the child learns to recognize and memorize the letters of the alphabet. Then, at the transitional level, the child learns to use the alphabet and principles of grammar and sentence structure to read and become literate. The ability to read is the foundation for further, specific learning. So too are security basics and literacy the foundation for further specific learning related to one's role(s) with respect to information systems.

Information security literacy must not be confused with the term "computer literacy," which refers to an individual's familiarity with a basic set of knowledge needed to use a computer. Information security literacy refers to an individual's familiarity with, and ability to apply, a core knowledge set (i.e., "information security basics") needed to protect information and systems. Just as computer literacy is a generic foundation, i.e., is not geared to specific technology or application(s), so too is information security literacy a one-size-fits-all foundation for further learning; it is not geared to any specific system. All individuals who use information or information systems, regardless of their specific job responsibilities, must know and be able to apply information security basics.

The Information Security Awareness Training: Basics and Literacy level has the following learning objectives:

- To ensure that users of information and information systems understand the core set of key terms and essential information security concepts that are fundamental for the protection of information and information systems. Many of the terms and concepts should have been previously introduced in an agency's awareness briefing or other basic awareness activities. In that case, information security basics and literacy provides reinforcement and structure.

- To promote personal responsibility and positive behavioral change throughout an organization's information and information system user population, beyond what is disseminated in the organization's basic awareness efforts.

- To offer an information security awareness training curriculum framework to promote consistency across government.

These objectives are designed to permit a consistent, government-wide approach to ensure that all users who are involved with information systems, regardless of agency, organizational unit, role(s), or specific system(s), acquire comparable and comprehensive literacy in information security basics. The value of such a consistent training program is the portability of information security literacy as employees change jobs and organizations.

3.2. Basics – Core Set of Information Security Terms and Concepts

The body of knowledge associated with information security is large and growing at an increasing rate, commensurate with rapid technological changes. Regardless of its size and growth rate, certain basic terms and concepts form the foundation of any effective information security program and environment. These terms and concepts must be learned and applied as the individual proceeds from information security awareness to awareness training to role-based training. The terms and concepts related to information security awareness training basics and literacy are those that support an understanding of the topics listed below in a curriculum framework designed for all users.

3.3. Literacy – Curriculum Framework

The awareness training literacy level is the first solid step in information security learning, where the obtained knowledge can be directly related to the individual's role as "user" in his or her organization. Although the curriculum framework presented below provides a generic list of topics to be included in awareness training literacy courses, it is imperative that the actual course content reflect the organization's unique culture and mission requirements. Emphasis placed on the specific topics may vary by audience or organization needs.

The curriculum framework was developed by the Information Systems Security Line of Business (ISS LOB) Tier 1 Awareness Training Working Group, and was adopted by the Office of Management and Budget (OMB). The topics below represent the minimum topics that the ISS LOB Tier 1 Awareness Training Shared Service Centers (SSCs) have been instructed to incorporate into their awareness training products being developed for departments and agencies.[14]

The current list of topics includes:

- Roles and responsibilities in information security
- Ways to protect shared data (e.g., encryption, backups)
- Examples of internal and external threats (e.g., social engineering, hackers)
- Malicious code (e.g., viruses, worms)
- Security controls
- Ways to recognize an information security incident
- Principles of information security
- Passwords
- Social engineering
- Data backup and storage
- Computer viruses and worms
- Incident response
- Personal use and gain
- Privacy
- Personally identifiable information (PII)
- Identity theft
- Internet surfing

---

[14] As the list of minimum topics to be included in awareness training material developed by SSCs will certainly change over time, NIST will augment this list online at http://csrc.nist.gov. Conversely, the federal government's program manager or program office that is responsible for implementing, monitoring, and maintaining the ISS LOB Tier 1 Awareness Training initiative may develop and maintain a list of minimum topics.

- Inventory control
- Physical security
- Spyware
- Phishing
- Scams and spam
- Mobile devices (e.g., laptops, PDAs)
- Portable storage devices (e.g., CDs, USB drives)
- Remote access
- Copyright infringement and software piracy
- Use and abuse of e-mail
- E-mail do's and don'ts
- Peer-to-peer file sharing threats
- National security information/systems, where applicable

Organizations, including SSCs, are encouraged to also include the following topics:

- Consequences of user actions
- Use and abuse of all/any systems and/or applications, not just e-mail
- Prohibited use (e.g., downloading/viewing pornography, gambling)
- Help desk reference
- Links to policies (e.g., federal, department, agency, local)

There are a variety of suitable approaches for teaching this subject matter. One of the most effective is to encourage participation by the students in interactive discussions on how the various topics and concepts relate to their particular organization or jobs. This approach allows users to understand the significance of information security principles and procedures to their organization, and to begin finding ways of applying this new knowledge in their work environment. Some organizations will opt to present this information security awareness training basics and literacy material to their user populations using web-based or computer-based technologies.

Organizations may have a need to develop a more complex information security awareness training course. This need may arise over time as the user population "outgrows" the basic awareness training course. Similarly, repeating the same or similar information year after year will desensitize users, resulting in less effective training. The need for a more complex awareness training course may also arise as a result of the makeup of the user population. Some organizations have a technology-focused workforce and/or a research-oriented workforce that might have to be challenged by a more complex course.

The information security training topics and elements listed in Exhibit 4-4 of the next chapter can be used to develop a more complex awareness training course. Although these topics and elements are key parts of the role-based training methodology, they can be used to craft an appropriate awareness training course.

The recommendations presented in this chapter are designed to assist organizations in meeting their information security awareness training responsibilities for users of information and information systems. This material is not a substitute for role-based training. Although some of the topics in the list above appear to be similar to some of the topics and elements presented

> An awareness training course is not a substitute for role-based training.

in the next chapter as building blocks for role-based training, the coverage of material in role-based courses is at a greater depth and is tailored for each role, compared to the one-size-fits-all level of coverage designed here for users of information and information systems.[15]

Beginning in Chapter 4, a methodology for development of role-based training is presented to provide for the in-depth training requirements of individuals who have been identified as having significant responsibility for information security.

---

[15] In the April 1998 publication of NIST SP 800-16, "user" was one of the 26 roles described in the role-based training methodology. With the advent of the "awareness training" term, the role of "user" has, for all practical purposes, been moved out of the list of potential roles for role-based training, and moved to the Information Security Awareness Training: Basics and Literacy level of the Learning Continuum.

Chapter 4

4. Implementing Role-Based Training

A companion publication to this document, NIST Special Publication 800-50, *Building An Information Technology Security Awareness and Training Program*, provides guidelines for building an effective information security awareness and training program and supports related requirements in FISMA, OMB Circular A-130, Appendix III, and OPM's 5CFR Part 930.

NIST SP 800-50 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.[16]

This chapter begins with a discussion about utilizing the results of the agency-wide needs assessment. (A necessary assumption is that the needs assessment identified that role-based training needs to be developed for a role or multiple roles, or that existing training needs to be enhanced.) This chapter will introduce the instructional systems design (ISD) process known as **ADDIE** (**A**nalysis, **D**esign, **D**evelopment, **I**mplementation, and **E**valuation). This chapter will also identify and describe each of the components that make up the role-based training methodology, and will describe how each component is used to develop the role-based information security training course or module identified in the needs assessment.

4.1. Utilizing the Needs Assessment

Figure 4-1 shows the relationship between identified role-based training requirements and an organization's current efforts. The shaded area represents the additional security training efforts that need to be made. The needs assessment helps identify these additional needs – the gap between what is currently being done and what is required.

---

[16] Although NIST SP 800-50 addresses and describes an information security awareness and training needs assessment, because the focus of this chapter is limited to role-based training, only the training aspect of an awareness and training needs assessment and the awareness and training program is discussed here.
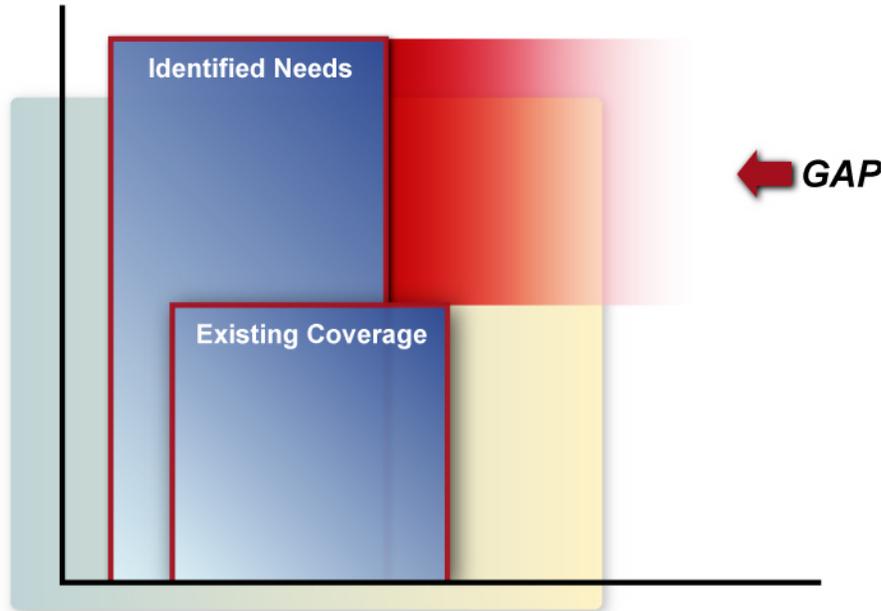
Figure 4-1: Required Role-Based Training versus Current Effort

Another important result of the needs assessment is the related information security 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.

4.1.1. Setting the Bar

"Setting the bar" means that a decision must be made as to the complexity of the material that will be developed. The complexity must be 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: 1) the target attendee's position within the organization, and 2) knowledge of the security skills required for that position. The complexity of the material must be determined before development begins. Setting the bar is an important aspect of the "scoping guidance" to be developed and utilized throughout the ADDIE process.[17]

4.2. Role-Based Training

The Learning Continuum presented in Chapter 2 shows the relationship between awareness, awareness training (security basics and literacy), role-based training, and education. The Continuum demonstrates that awareness and awareness 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, information security training is to be provided to individuals based on their particular roles and information security responsibilities, especially if they have been identified as having significant responsibility for

---

[17] "Scoping guidance" was first used in NIST SP 800-53. Here, in the context of role-based training, "scoping guidance" is used to describe the flexibility an organization has to build, or have built, information security courses or modules, using the results of needs assessments, job task analyses, and the training methodology described in this chapter.

information security. Information security-focused education is intended for designated information security professionals in addition to role-based training.[18]

4.3. Role-Based Training Versus Topic-Based Training

Role-based training allows the recipient of training to learn what he or she needs to know and be able to do, based on their current job. This is perhaps the most important distinction between role-based and topic-based training. 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 information security training can in itself be 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 are 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, and therein lies the problem with most topic-based training. For example, "generalists" – 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" – 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.[19]

4.4. Understanding the Role-Based Training Methodology

The role-based training methodology that is described in this chapter is easy enough to understand, but only if the relationships between the various parts of the methodology are understood. These parts include the a catalog of roles, role-based training matrices, functional responsibilities, training areas, cells, cell description modules, and the information security training topics and elements. These parts, or building blocks, are described in the remainder of this section.

4.4.1. Roles

Over time, individuals acquire different roles relative to their use of information and information systems and applications. Roles change as an individual progresses through his or her career, either within an organization, or as they make a career move to a different organization. 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

---

[18] While many information security professionals, and others whose roles require some role-based security training, enter the workforce with a formal education foundation, "education" as used here and in the Learning Continuum is meant to address the additional formal information security-focused education that can be obtained to augment role-based training and experience.

[19] There are noteworthy exceptions to the built-in problem of topic-based training. Companies that focus their training on a particular role often offer topic-based training that is tailored to the needs of that role. In these cases, training aimed at, for example, administrators of particular operating systems and/or platforms looks and feels far more like role-based training than typical topic-based training. Organizations that build topic-based training for their employees often know which roles will be represented in either one-time training offerings or recurring training sessions. They can add pointers or emphasis to various topics, stating for what role or roles particular material applies. Courses can also be organized such that more general information is presented early for roles that have more management responsibilities, while more in-depth topics are covered later for later-arriving staff with more technical responsibilities.

board to evaluate vendor proposals for information systems. The information security 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 responsibility for information security.

The roles listed and described in this document carry varying degrees of responsibility for information security, 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 security responsibility than will a person serving in another role. A person in one role will also need to know more about some aspects of information security than will a person serving in another role. For example, a CIO or SAISO/CISO will need to know more about federal laws and regulations and department/agency policy than will a system administrator. They will need to know more about managing an information security 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 material should be considered to be included in a training course or module for each role.[20]

The training methodology described in this chapter focuses on providing the instructional design specialist (IDS) with the tools to build a course or module based on the information security role of the intended audience. Exhibit 4-1 is a list of those roles that are more than likely going to be identified by one organization or another as having significant responsibility for information security. To be clear, the list of roles is provided here - and a corresponding list of role-based training matrices is in Appendix A - to simply show the reader what roles have been identified and have been described later in this chapter and document for use by an IDS.

> The roles listed in Exhibit 4-1 are to be viewed as a catalog. There is no requirement that mandates, and no recommendation that suggests that training courses or modules be built for all the roles shown.

---

[20] Although various organizations may use the same role name to describe or label people who do similar work, the actual knowledge, skills, and abilities needed by incumbents in same-titled positions may vary from organization to organization, and even within the same department or agency. A needs assessment conducted across an organization will identify groups of people who need information security training. 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.

- Agency Head and Other Executives
- Assessor
- Auditor, External
- Auditor, Internal
- Authorizing Official
- Chief Information Officer (CIO)
- Contracting Officer
- Contracting Officer's Technical Representative (COTR)
- Data Center Manager
- Database Administrator
- First Responders
- Freedom of Information Act Official
- Incident Response Coordinator
- Information Owner
- Information Resources Manager
- Information System Security Officer (ISSO)
- Network Administrator / Network Security Specialist
- Office of General Counsel Staff
- Privacy Act Official
- Program and Functional Managers
- Programmer / Systems Analyst
- Risk Executive
- Risk / Vulnerability Analyst
- Security Administrator
- Security Engineer
- Senior Agency Information Security Officer (SAISO) / Chief Information Security Officer (CISO)
- Senior Information Resources Management Official
- Source Selection Board Member
- System Administrator
- System Designer / Developer
- System Operations Personnel
- System Owner
- Technical Support Personnel
- Telecommunications Personnel

Exhibit 4-1: Catalog of Roles

This list should be seen as a catalog, the place in this document where an organization and/or an IDS would begin the process to develop training material for a course or module.[21] It is important to understand that just because a role is listed in Exhibit 4-1, it does not mean that a training course or module must be built for that role. Training must be developed (or purchased) and provided if no such training exists for a role, if the organization has identified that role as

---

[21] The identification of a role or roles in need of training would be accomplished by: 1) a needs assessment, 2) an inspector's review, or 3) the person or people in the organization tasked with identifying those with significant responsibilities for information security. These processes can also identify whether training is to be developed where none exists for a role or roles, or if existing training needs to be updated. Regardless of how roles are identified for information security 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 information security training function, supervisors can determine if the needed training is available in-house, or must be sought elsewhere.

having significant responsibility for information security.[22] Existing training must be enhanced and provided if a needs assessment and/or job task analysis indicates that current training is not meeting the information security needs of the intended audience.

> Training must be developed (or purchased) and provided if no such training exists for a role, if the organization has identified that role as having significant responsibility for information security.

## 4.4.2.	The Information Security Training Matrix

For each of the roles listed in Exhibit 4-1, there is a corresponding role-based matrix in Appendix A. A sample non-role-specific matrix is shown below as Exhibit 4-2. The design of the matrix is related to the Training level of the Learning Continuum on Page 12. The matrix is a key part of the role-based training methodology. In turn, the matrix contains other elements, the understanding of which is important to understanding and using this methodology. These elements within each matrix are:

- Organizational responsibilities,
- Training areas, and
- Cells.

Each of these elements is described in detail in the following subsections.

Role: _____					
	Responsibilities				
Training Areas	**A Manage**	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C	■■■■	3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A	■■■■		3.5D	3.5E

Exhibit 4-2 Information Security Training Matrix

---

[22] There may be instances in which some people in a role, but not all, are identified as having significant responsibility for information security. 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 security 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 responsibility for information security, 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.

4.4.3. Organizational Responsibilities

An individual's need for information security training changes 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. Several roles in Exhibit 4-1 - Agency Head, CIO, and System Owner - will generally have more management responsibility and less technical responsibility. Contracting Officers and Contracting Officer's Technical Representatives (COTRs) will have more acquisition-related responsibilities and fewer management-oriented or technically oriented responsibilities. Some roles, like Technical Support Personnel, System Operations Personnel, System Administrator, and Network Administrator, will have more technical responsibilities and far less management responsibilities.[23] Others, like Agency Head and Other Executives, Auditors, and Risk Executives, will have more oversight responsibilities.

The training methodology described in this document is flexible in its accounting for the various responsibilities found in a role, or across many roles. This need for flexibility in the training methodology is first reflected in the Learning Continuum by segmenting the Training Level (see Page 12) into five generic organizational responsibilities. These responsibilities are:

- Manage,
- Acquire,
- Design and Develop,
- Implement and Operate, and
- Review and Evaluate.

These five responsibilities are key elements in the training matrix.

In the matrix, the five responsibilities are found in columns. Each column is labeled with not only the responsibility, but with a letter - A through E – that is tied to the responsibility. In Exhibit 4-2 and in each matrix in Appendix A, the responsibility of Manage is always tied to column A. Acquire is always linked to column B. Design and Develop is always associated with column C, and so on. The importance of this detail becomes clearer in the next subsection.

The five responsibilities have a definite working relationship with another element of the matrix – training areas. The training areas element is discussed next.

4.4.4. Training Areas

There are three training areas, or training content areas, in the matrix. They are located in a column on the left side of the sample matrix in Exhibit 4-2, and in each role-specific matrix in Appendix A. The training areas are:

- Laws and Regulations,
- Security Program, and
- System Life Cycle Security.

---

[23] While a system administrator may have more technical responsibilities as he or she gains experience and is promoted to a journeyman level of proficiency, if that person becomes a supervisor or manager and leads a staff of more junior personnel, this more mature role would include more management responsibilities. The training methodology described in the chapter is flexible enough to allow the IDS to build a course or module that reflects this change in role-related responsibilities over time.

The training areas, when viewed relative to the responsibilities, begin to indicate to the IDS what kind of information will be included at the intersection of a training area and a responsibility that applies to the role for which they are building a training course or module.[24]

Generally speaking, the three training areas include:

- Laws and Regulations—the types of knowledge, skills, and abilities (KSAs) relative to the laws and regulations pertaining to the protection of information and information systems that govern the management and use of systems within the federal government. These include government-wide requirements such as FISMA and other applicable laws; policy promulgated by the Office of Management and Budget in the form of bulletins, memoranda, and other documents that levy information security-related responsibilities on federal organizations; standards and guidelines disseminated by NIST; as well as policies and procedures specific to the department or agency developing or purchasing role-based training;

- Security Program— KSAs relative to the establishment, implementation, maintenance, and monitoring of an information security program within an organization; and

- System Life Cycle Security— KSAs relative to information security needed throughout each phase of a given system's life cycle. In this instance, a five-phased system life cycle model is used (i.e., initiation, development/acquisition, implementation/assessment, operations/maintenance, and disposal).

In the column that lists the training areas note that each of the three areas is numbered. Two areas have sub-areas or sub-elements and these are also numbered. For example, under the training area called Security Program are two sub-areas: Planning is numbered 2.1, while Management is numbered 2.2. Each of the five phases of the training area System Life Cycle Security are also numbered.

At the intersection of each vertically aligned responsibility and each horizontally aligned training area is a "cell." Cells contain information about training areas, relative to specific responsibilities that apply to roles. Each training area row carries a number and each responsibility column carries a letter in order for each cell to be labeled with a distinctive number-letter label, making it easy to identify and use each cell. Cells are discussed in greater detail in the following subsection.

> At the intersection of each vertically aligned responsibility and each horizontally aligned training area is a "cell."

4.4.5. Cells

Each matrix contains 37 cells, in that there are 37 places in the matrix where responsibility columns intersect training area or sub-area rows. Cells are logical places in the matrix where those in a role that has an emphasis on a particular responsibility need to know related information contained in one of the training areas. For example, training courses or modules for people in roles that involve primarily management functions (e.g., Agency Head, CIO, SAISO/CISO) will have particular cells in the Manage column selected in the role-specific matrix in Appendix A. Those cells – including Cell 1A, for example – will identify training areas about which the target audience will need to know something. In the example of Cell 1A, audience members will need to know about federal laws and regulations, department and agency policy, and applicable standards and guidelines. The exact information and the depth of coverage of topics is determined by a combination of the results of a job task analysis, the complexity of the course or module (i.e., beginning, intermediate, advanced), and the audience's needs in a particular training session.

---

[24] This intersection of a training area with a responsibility is discussed in far greater depth in the next two subsections.

> Cells are logical places in the matrix where those in a role that has an emphasis on a particular responsibility need to know related information contained in one of the training areas.

While there are 37 cells for which there is a logical intersection of responsibility columns and training area rows, there are three spaces or non-cells in Exhibit 4-2 and in each matrix in Appendix A which are not used.   These are excluded in the matrices because there is no instance, or usually no instance, in which there would be a responsibility that would have a need for a particular training area. For example, consider the intersection of responsibility Column B (Acquire) and training area 3.5 (Disposal). It is unlikely that someone in a role who has acquisition responsibility is going to need training in how to acquire some good or service during the disposal phase of an information system. Similarly, someone in a role who has some responsibility to design and develop (Column C) will probably not have to learn how to design and develop some aspect of a system going through its disposal (Row 3.5) phase.[25]

Although there are 37 cells available in each matrix, not including the three aforementioned non-cells, only specific cells are included in each matrix in Appendix A. The cells identified in each matrix represent typical pairings of role responsibilities and training areas, based on feedback from role-specific working groups. The number of cells and the selection of specific cells in each matrix is directly related to the kind of information that each audience needs, emphasizing one or more of the training areas, and focusing on the responsibilities of a person with that role. For example, a matrix for the role of Auditor (Internal or External) shows a total of eleven cells selected, including all the cells in the Review and Evaluate column (Column E). This reflects the nature of the

> The cells identified in each role's matrix in Appendix A are recommendations, and are to be considered a starting point when first looking at a role-specific matrix, prior to developing a training course or module.

work that a typical information security auditor does - they inspect the various aspects of an information security program, often including the life cycle phases of a system's or application's development. By contrast, a matrix for the role of Contracting Officer has seven cells selected, and all seven are in the Acquire column (Column B). This is consistent with the information security responsibility of the typical contracting officer being limited to acquisition. Contrast this with the number of cells selected for the typical SAISO/CISO. In the matrix for this role, all cells are selected as a starting point, because the typical SAISO or CISO must know something about each training area and (usually) has some responsibility across each of the responsibility columns.

The cells identified in each role's matrix in Appendix A are recommendations, and are to be considered a starting point when first looking at a role-specific matrix, prior to developing a training course or module. The number of cells can be increased or decreased, depending on the training needs of an organization. The number of cells can be increased or decreased if more or fewer training areas are needed and if more or fewer responsibilities are needed for a given role. It is the results of a job task analysis performed on a group of people in a role that identifies the specific training needs of people in that role. The results of the job task analysis should be used to fine-tune the matrix for a role, adding or deleting cells as needed.

> It is the results of a job task analysis performed on a group of people in a role that identifies the specific training needs of people in that role.

Cells are the building blocks that make up training courses or modules. If the IDS, or the IDS working with information security professionals, serving as subject matter experts, know what

---

[25] If an organization has a need to provide training relative to responsibilities that intersect training areas in any or all three of the three non-cells, the methodology is flexible enough to allow the conversion of each non-cell into a cell.

material is needed to populate each cell to be used in a training course or module, they can begin building the course or module, cell by cell. However, if additional information is needed to begin to populate each cell with material, continue reading about cell description modules and the information security training topics and elements. How material is developed for each cell is described in the next subsection.

4.4.6.   Cell Description Modules

Each cell in a matrix in Appendix A has a corresponding cell description module or sheet – cell description pages - in Appendix B. The cell description contains information that is critical for an IDS to know when building a course. Each cell description module identifies the applicable training area and responsibility (e.g., manage, acquire, design and develop). Each cell description module also includes:

- the definition of the function of the cell as the intersection of a responsibility column and a training area row,

- the behavioral outcome that the material built for that cell should produce in the training course or module recipient,

- knowledge levels (i.e., beginning, intermediate, advanced),

- terminal learning objectives for each of the three possible knowledge levels, and

- specific information security-related topics from the information security training topics and elements exhibit that apply to that cell.

The format of a cell description module is contained in Exhibit 4-3.

With the information contained in each cell description module or sheet, the IDS can begin to build training material that will make up the role-based training course or module.

<div style="border: 2px solid black; padding: 1em;">

<div style="background-color: #d9d9d9; padding: 0.5em;">

INFORMATION SECURITY TRAINING
Responsibility-Based Curriculum Outline Module
Training Area (#)

Training Area: **(Sub Area)**
Responsibility: **Manage**

</div>

Definition —

Behavioral Outcome —

Knowledge Levels — (keywords)

1. Beginning — (Research, Know, Identify)
2. Intermediate — (Analyze, Understand, Apply)
3. Advanced — (Interpret, Approve, Decide, Issue)

Terminal Learning Objectives — (at each level)

At the conclusion of this module, individuals will be able to:

1. Beginning —
2. Intermediate —
3. Advanced —

Applicable Roles (minimum) — (list each applicable role)

</div>

Exhibit 4-3: Cell Description Module Format

Aspects of the cell description module are:

- Title Block — Labels the cell within the matrix and identifies the specific training area and responsibility addressed.

- Definition — Defines the training area addressed.

- Behavioral Outcome — Describes what an individual who has completed the specific training module is expected to be able to accomplish in terms of information security-related job performance.

- Knowledge Levels — Provides verbs that describe actions an individual should be capable of performing on the job after completion of the training associated with the cell. The verbs are identified for three training levels: Beginning, Intermediate, and Advanced.

- Terminal Learning Objectives — Links the verbs from the Knowledge Levels section to the Behavioral Outcomes by providing examples of the activities an individual should be capable of doing after successful completion of training associated with the cell. Again, the Learning Objectives recognize that training will be provided at beginning, intermediate, or advanced levels. For some of the cells, there will not be three distinct

levels (i.e., there may be only two levels or even one). In these instances, there is no clear distinction between performance objectives that allows separation into beginning, intermediate, and advanced levels. (Note: Beginning, intermediate, and advanced refer to levels of information security responsibility associated with the functional area, not to levels of the functional area as such. For example, an experienced (advanced level) system developer could be taking entry-level (beginning) training in the information security responsibilities associated with the system development function.) The purpose of the beginning level is to focus the generic understanding of information security, which the individual will have acquired from Awareness Training: Basics and Literacy (see Chapter 3), on their job requirements.

- Roles — Presents a list of roles for which the described cell is included as a recommended starting point for consideration by the IDS. Whether the cell is actually used in a training course or module is determined in part by a job task analysis.

4.4.7.   Information Security Training Topics and Elements

Once the selection of cells to be used in an information security course or module is finalized, the IDS should focus on the recommended information security training topics that are listed on the second page of each cell description module or sheet.

As shown in Exhibit 4-4, there are 12 topics. In turn, each topic has a set of related elements. Each cell description module has particular topics, or in some cases, has all 12 topics identified for use, or for consideration for use.

> Only those elements that allow the training recipient to meet the terminal learning objectives and behavioral outcome for each cell are to be selected from each topic.

While it may not be immediately clear why the same topic number appears in a number of cells, the IDS must understand that there are elements in each of the called-out topics that are to be used, or can be used, to develop training material for each specified cell. Only those elements that allow the training recipient to meet the terminal learning objectives and behavioral outcome for each cell are to be selected from each topic. For example, regarding the roles of CIO and System Owner, in the matrix for each role in Appendix A, cell 2.1A is shown as one of the cells called out for initial consideration for each role. (Cell 2.1A is the intersection of the Manage responsibility and the Security Program – Planning training area.) Within cell 2.1A, all 12 topics are called for to develop training material. This means that some elements of each of the 12 topics should be included when developing material for that module of the training courses for these respective roles. Only those elements that support the aforementioned "meet the terminal learning objectives and behavioral outcome" rule should be included when developing material.

Related to the discussion of using particular elements of a topic in the development of a cell's worth of training material is the alternative grouping of related material in a course or module. Although the structure of this training methodology indicates that a cell's worth of material would consist of particular elements from particular topics, the organization has complete freedom to structure the course or module as they deem appropriate.[26]

> The organization has complete freedom to structure the course or module as they deem appropriate.

This means that instead of addressing elements related to topic number 4 (System Interconnection) in nine different cells (i.e., 2.1A, 3.2A, 3.3A, 3.4A, 3.1B, 3.1C, 2.2D, 3.1E, 3.3E) or modules in a course for system owners [see Appendix A, Page A-12],

---

[26] A role-based information security training course or module can be organized by training area, responsibility, topic, or cell, using the methodology contained in this document.

a course could be organized such that system interconnection is addressed once in the course, but with appropriate mention of the various training areas and responsibilities in which system interconnection plays a part.

Similarly, and focusing on the role of system owner again, topic number 12 (Technical Controls) can be addressed once, with appropriate mention of the training areas and responsibilities in which technical controls play a part, rather than mentioning the appropriate elements of the topic in the ten cells (i.e., 2.1A, 3.3A, 3.4A, 3.1B, 3.3B, 3.4B, 2.2D, 3.1E, 3.2E, 3.3E) in which technical controls appear in the Appendix A matrix for System Owner.

The topics listed in Exhibit 4-4, used throughout the role-specific matrices in Appendix A, and listed in each cell description page in Appendix B cover information security program-level issues as well as system-level information. In many cases in Exhibit 4-4 and Appendix B, specific controls or control families from NIST Special Publication 800-53 are shown along with elements in the 12 topics. In some cases, other NIST publications are cited.[27]

---

[27] There are other valid sources of topics and elements which can be incorporated into role-based training courses. These include the Committee on National Security Systems (CNSS) training standards, the Department of Homeland Security (DHS) Essential Body of Knowledge (EBK), the OPM 2210 training competencies and topics project, the still-being-developed CIO Council's IT Workforce Committee's Information Security Training Matrix Project, and work in cyber security being done by the Office of the Director of National Intelligence (ODNI).

Information Security Training Topics and Elements
This exhibit presents a comprehensive body of knowledge – topics and elements – used in the information security field. It was developed by comparing, categorizing and combining topics, terms, concepts, and subjects from the following sources: NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*; NIST SP 800-100, *Information Security Handbook: A Guide for Managers*; *Federal Information Security Management Act of 2002* (FISMA); and OPM 5 CFR Part 930, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems* (June 2004).

1. LAWS AND REGULATIONS
Federal government-wide and organization-specific laws, regulations, policies, guidelines, standards, and procedures mandating requirements for the management and protection of information technology resources.

Elements: **LR-a** Federal Laws, Regulations, Standards, and Guidelines
             LR-b Legal and Liability Issues
             LR-c Organization Policy, Guidelines, Standards and Procedures Life Cycle Support
             LR-d System-specific Policy, Guidelines, Standards and Procedures

<u>**Additional Reference**</u>: **NIST SP 800-53 (XX-1 for all control families)**

2. INFORMATION SECURITY PROGRAM
A program established, implemented, and maintained to assure that adequate Information Security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its general support systems and major applications.

Elements: **ISP-a** Organization-wide Information Security Program
             ISP-b System-level Information Security Program
             ISP-c Roles, Responsibilities, and Accountability
             ISP-c1 Senior Management
             ISP-c2 Organization-wide Information Security Managers
             ISP-c3 Program and Functional Managers
             ISP-c4 System/Application Owners
             ISP-c5 Information Owner/Custodian
             ISP-c6 IT System Security Managers
             ISP-c7 Contractors
             ISP-c8 Related Security Program Managers
             ISP-c9 Users

<u>**Additional Reference**</u>: **NIST SP 800-100**

3. SYSTEM ENVIRONMENT
The unique technical and operating characteristics of an IT system and its associated environment, including the hardware, software, firmware, communications capability, and physical location.

Elements: **SYSE-a** IT Architecture
SYSE-b Hardware Types
SYSE-c Operating Software
SYSE-d Application Software
SYSE-e Communication Requirements
SYSE-f Facilities Planning
SYSE-g Processing Workflow
SYSE-h Utility Software
SYSE-j Associated Threats
SYSE-k Associated Vulnerabilities

Additional Reference: NIST SP 800-53 (Control Families PE and SC)

---

4. SYSTEM INTERCONNECTION
The requirements for communication or interconnection by an IT system with one or more other IT systems or networks, to share processing capability or pass data and information in support of multi-organizational or public programs.

Elements: **SYSI-a** Network Architecture
SYSI-b Electronic Mail
SYSI-c Electronic Commerce
SYSI-d Electronic Funds Transfer
SYSI-e Electronic Data Interchange
SYSI-f Digital Signatures
SYSI-g Communications Types
SYSI-h Access Controls (e.g., firewalls, proxy servers, dedicated circuits)
SYSI-j Monitoring
SYSI-k Cryptography

Additional Reference: NIST SP 800-53 (Control Families AC, IA and SC)

---

5. INFORMATION SHARING
The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.

Elements: **INFO-a** Network Architecture
INFO-b Electronic Mail
INFO-c Electronic Commerce
INFO-d Electronic Funds Transfer
INFO-e Electronic Data Interchange
INFO-f Digital Signatures
INFO-g Communications Types
INFO-h Access Controls (e.g., Firewalls, Proxy servers, Dedicated circuits)
INFO-j Monitoring
INFO-k Cryptography

INFO-m Data Ownership
INFO-n Data Storage Media Labeling and Protection

<u>**Additional Reference:**</u> **NIST SP 800-53 (Control Families AC, IA, MP and SC)**

6. SECURITY OBJECTIVES

An IT environment consists of the system, data, and applications which must be examined individually and in total. All IT systems and applications require some level of protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the sensitivity and criticality of the information processed, the relation of the system to the organization missions and the economic value of the system components.

<u>**Elements:**</u>   **SENS-a** Confidentiality
SENS-b Integrity
SENS-c Availability

<u>**Additional Reference:**</u> **NIST SP 800-53 (Control Families CA and RA)**

7. RISK MANAGEMENT

The on-going process of assessing the risk to IT resources and information, as part of a risk-based approach used to determine adequate security for a system, by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

<u>**Elements:**</u>   **RISK-a** Risk Assessment
RISK-b Risk Analysis
RISK-c Risk Mitigation
RISK-d Uncertainty Analysis
RISK-e Threats
RISK-f Vulnerabilities
RISK-g Risks
RISK-h Probability Estimation
RISK-j Rate of Occurrence
RISK-k Asset Valuation
RISK-m Adequate and Appropriate Protection of Assets
RISK-n Cost Effectiveness
RISK-p Cost-Benefit Analysis
RISK-q Application Security Reviews/Audits
RISK-r System Security Reviews/Audits
RISK-s Verification Reviews
RISK-t Internal Control Reviews

<u>**Additional Reference:**</u> **NIST SP 800-53 (Control Families AU, CA, CP, IR and RA)**

8. MANAGEMENT CONTROLS

Management controls are actions taken to manage the development, maintenance, and use of the

system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions.

Elements: **MGMT-a** System/Application Responsibilities
              MGMT-a1 Program and Functional Managers
              MGMT-a2 Organization-wide Information Security Managers
              MGMT-a3 Owners
              MGMT-a4 Custodians
              MGMT-a5 Contractors
              MGMT-a6 Related Security Program Managers
              MGMT-a7 IT System Security Manager
              MGMT-a8 Users
              MGMT-b System/Application-Specific Policies and Standard Operating Procedures
              MGMT-c Personnel Security
              MGMT-d Background Investigations
              MGMT-e Position Sensitivity
              MGMT-f Separation of Duties/Compartmentalization
              MGMT-g System Rules of Behavior
              MGMT-h Assignment and Limitation of System Privileges
              MGMT-j Individual Accountability
              MGMT-k Sanctions or Penalties for Violations
              MGMT-m Connection to Other Systems and Networks
              MGMT-n Intellectual Property/Copyright Issues
              MGMT-p Remote Access/Work at Home Issues
              MGMT-q Official vs. Unofficial System Use

Additional Reference: NIST SP 800-53 (Control Families MA, PS and PL)

---

9. ACQUISITION/DEVELOPMENT/INSTALLATION/IMPLEMENTATION CONTROLS
The process of assuring that adequate controls are considered, evaluated, selected, designed and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation and operation stages.

Elements: **ADII-a** Life Cycle Planning
              ADII-b Security Activities in Life Cycle Stages
              ADII-c Security Plan Development and Maintenance
              ADII-d Security Specifications
              ADII-e Configuration Management
              ADII-f Change Control Procedures
              ADII-g Design Review and Testing
              ADII-h Authority to Operate
              ADII-j Certification/Recertification
              ADII-k Accreditation/Re-accreditation
              ADII-m Acquisition Specifications
              ADII-n Contracts, Agreements, and Other Obligations
              ADII-p Acceptance Testing

ADII-q Prototyping

Additional Reference: NIST SP 800-53 (Control Families CM, PL and SA)

10. OPERATIONAL CONTROLS

The day-to-day procedures and mechanisms used to protect operational systems and applications. Operational controls affect the system and application environment.

Elements: **OPS-a** Physical and Environmental Protection
OPS-b Physical Security Program
OPS-c Environmental Controls
OPS-d Natural Threats
OPS-e Facility Management
OPS-f Fire Prevention and Protection
OPS-g Electrical/Power
OPS-h Housekeeping
OPS-j Physical Access Controls
OPS-k Intrusion Detection/Alarms
OPS-m Maintenance
OPS-n Water/Plumbing
OPS-p Mobile and Portable Systems
OPS-q Production, Input/Output Controls
OPS-r Document Labeling, Handling, Shipping and Storing
OPS-s Media Labeling, Handling, Shipping and Storing
OPS-t Disposal of Sensitive Materials
OPS-u Magnetic Remnants - Cleaning and Clearing
OPS-v Contingency Planning
OPS-w Backups
OPS-x Contingency/Disaster Recovery Plan Development , Testing, and Implementation
OPS-y Contracting for Contingency Services
OPS-z Contracting for Disaster Recovery Services
OPS-aa Insurance/Government Self-Insurance
OPS-bb Audit and Variance Detection
OPS-cc System Logs and Records
OPS-dd Deviations from Standard Activity
OPS-ee Hardware and System Software Maintenance Controls
OPS-ff Application Software Maintenance Controls
OPS-gg Documentation

Additional Reference: NIST SP 800-53 (Control Families AC, AU, CP, IA, IR, MA, MP and PE)

11. AWARENESS, TRAINING, AND EDUCATION CONTROLS

Awareness programs set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure. The purpose of *training* is to teach people the skills that will enable them to perform their jobs more effectively. *Education* is

targeted for information security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities.

Elements: **ATE-a** Awareness Activities
                ATE-b Awareness Training (Basics and Literacy)
                ATE-c Role-Based Training
                ATE-d Education
                ATE-e Certifications

Additional Reference: NIST SP 800-53 (Control Family AT)

---

12. TECHNICAL CONTROLS
Technical controls consist of hardware and software controls used to provide automated protection to the IT system or applications. Technical controls operate within the technical system and applications.

Elements: **TECH –a** User Identification and Authentication
               TECH –b Passwords
               TECH –c Tokens
               TECH –d Biometrics
               TECH –e Single Log-in
               TECH –f Authorization/Access Controls
               TECH –g Logical Access Controls
               TECH –h Role-Based Access
               TECH –j System/Application Privileges
               TECH –k Integrity/Validation Controls
               TECH –m Compliance with Security Specifications and Requirements
               TECH –n Malicious Program/Virus Protection, Detection and Removal
               TECH –p Authentication Messages
               TECH –q Reconciliation Routines
               TECH –r Audit Trail Mechanisms
               TECH –s Transaction Monitoring
               TECH –t Reconstruction of Transactions
               TECH –u Confidentiality Controls
               TECH –v Cryptography
               TECH –w Incident Response
               TECH –x Fraud, Waste, and Abuse
               TECH –y Hackers and Unauthorized User Activities
               TECH –z Incident Reporting, Investigation, and Prosecution
               TECH –aa Public Access Controls
               TECH –bb Access Controls
               TECH –cc Least Privilege

Additional Reference: NIST SP 800-53 (Control Families AC, AU, IA, IR and SI)

Exhibit 4-4: Information Security Training Topics and Elements

4.5. *The ADDIE Instructional Design Model*

Figure 4-2 presents the ADDIE Instructional Design Model. The ADDIE model is a systematic instructional design model consisting of five phases: Analysis, Design, Development, Implementation and Evaluation.[28] Each phase consists of outcomes that feed into the next phase in the model. Each of the phases is discussed in detail in this section. Input to the Analysis phase is the output of the needs assessment identifying the existing training gaps within the organization. As each role is analyzed attention should be paid to the cells, topics, and elements chosen for use within each role where the cell, topic, or element developed may become a module that is suitable for use within other role-based training that may be required. For example, many of the roles listed in Exhibit 4-1 and in Appendix A require some level of knowledge of federal laws, and department and agency policy. A single development effort with multiple modules that can be added and removed base on the audience could save significant development time.
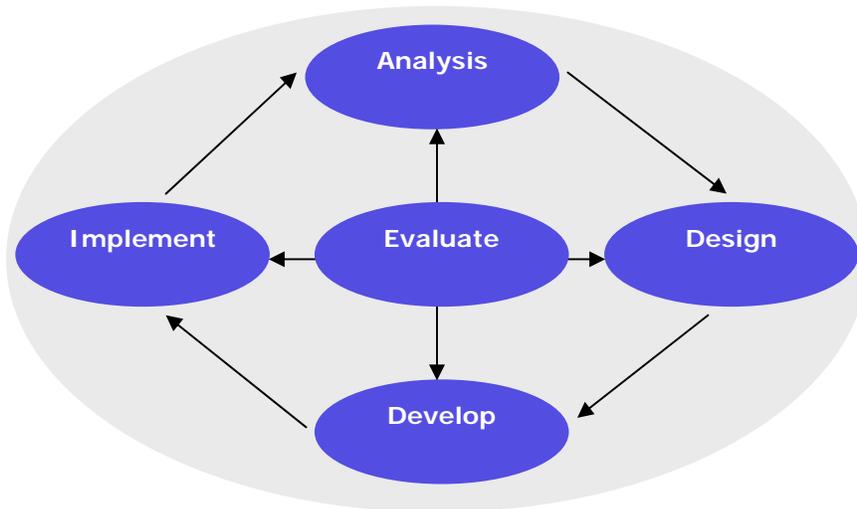
Figure 4-2: The ADDIE Instructional Design Model

4.5.1.   Analysis

During the Analysis phase, an inventory of all tasks associated with each role is compiled and the needs assessment is used to select those tasks for which training needs to be developed. Tasks can usually be found in position descriptions, performance plans, assignment letters, system security plans, and directives, or can be determined through interviews with current practitioners. Using these tasks, the IDS, with input from an information security SME, should:

- determine the knowledge level required

- develop desired behavioral outcomes, and

- develop performance measures for each task.

At this time it is also appropriate to determine if there is any prerequisite knowledge required for the training being developed. Appendix A, Role-based Training Matrices, can assist with the

---

[28] The ADDIE Model is an instructional design tool known to most IDSs. The model is briefly described in this section and used in Section 4.6 to illuminate its utility as part of the role-based training methodology described in this chapter and in Appendices A and B. If an information security professional or another non-IDS professional is tasked with developing role-based training, IDS training may be required.

identification of tasks. Appendix B, Information Security Training Curriculum Modules, contains behavioral outcomes for training developed for each cell used in each matrix.

As additional roles and their tasks are analyzed, the ISD can begin comparing these knowledge levels, behavioral outcomes, and performance measures to determine where training modules can be developed for multiple roles. The final step of the Analysis phase is to determine the instructional setting for the training (e.g. classroom, on-the-job, self-study, technology/computer-based training, etc.).

Figure 4-3 summarizes the steps of the Analysis phase.

Select Tasks to Train
Determine Knowledge Level Required
Develop Behavioral Outcomes
Develop Performance Measures
Determine Prerequisite Knowledge
Compare with other Training Required
Determine Appropriate Instructional Setting
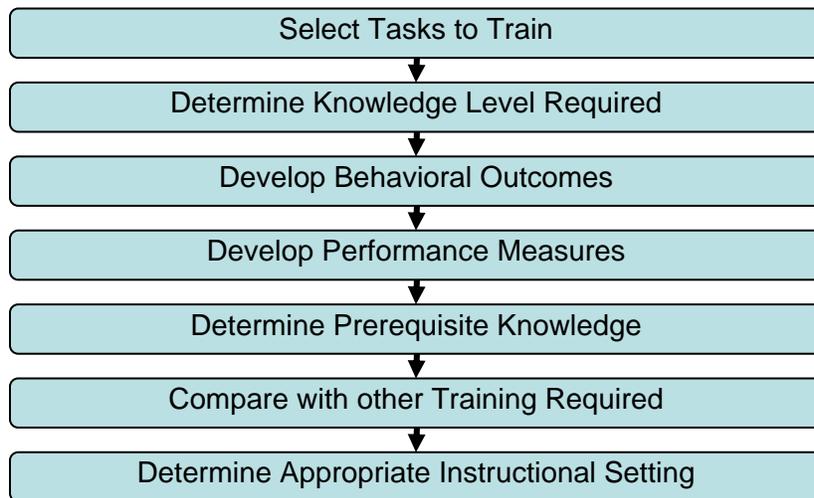
Figure 4-3: Analysis Phase

The outputs from the Analysis phase serve as the inputs to the Design phase and include role-specific tasks, knowledge levels, behavioral outcomes, performance measures and any required prerequisites.

4.5.2.   Design

The initial step of the Design phase is to develop the learning objectives for each of the tasks defined during the Analysis phase. Learning objectives include both terminal and enabling objectives. Appendix B contains terminal and enabling objectives for each cell used in each matrix.[29] From these objectives, the IDS should identify and list the steps required to accomplish each objective. These steps and objectives are then used to help develop the performance/knowledge tests required to show mastery of the objective. The prerequisite knowledge identified during the Analysis phase is then used to develop the entry behaviors that the training recipient must demonstrate prior to entering training.[30] The final step of the Design phase is to sequence the learning objectives. Sequencing typically orders objectives from easy to difficult. Care must be taken to ensure that all enabling objectives precede the terminal objective they support.

---

[29] Most of the cell description pages or modules in Appendix B include only the related terminal learning objectives. However, select cell description pages in the appendix also include enabling learning objectives. These select pages are for cells 1A, 2.1A, 2.2A, 3.1B, 3.2C, 3.3D, and 3.4E.

[30] Although developing required entry behaviors is a formal part of the Design phase of the ADDIE Model, an organization's information security training program may not require this step. Organizations may or may not develop and deploy pre-tests to gauge or verify the level of expertise that training recipients bring to the subject training.

Figure 4-4 summarizes the steps of the Design phase.
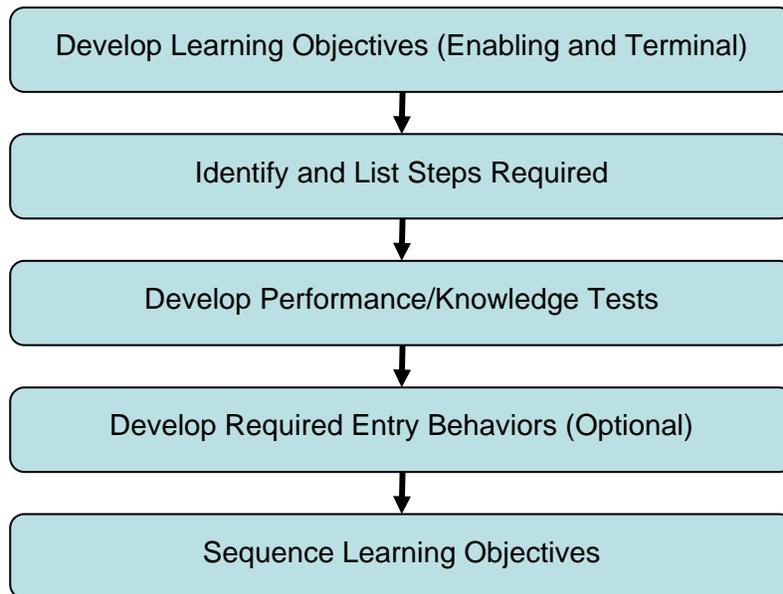
Figure 4-4: Design Phase

The Design phase outputs are a sequenced outline of the learning objectives to be covered in the course or module and preliminary performance and/or knowledge tests. These Design phase outputs are the primary inputs to the Development phase.

4.5.3. Develop

Using the sequenced outline of learning objectives, the IDS should identify and list the activities that will help the training recipients achieve each objective (e.g. lecture, simulation, role-play, demonstration, lab exercise, table-top exercise, etc.). The selected activities should result in the selection of an appropriate delivery method for presenting each of the objectives. Using the appropriate matrix in Appendix A for the role, determine the cells, topics, and elements needed and verify the knowledge level required for each learning activity identified. This is a good point to review any existing course material for possible reuse. The IDS should use the sequenced objectives, activities, and recommended cells, topics, and elements, to develop the course material to support the activities previously identified. Any performance tests identified during the Design phase should be incorporated in this phase. Once the course or module material is developed, lesson plans and an instructor guide should be assembled. The critical final step of the Development phase is to have all course/module materials reviewed and validated by someone knowledgeable in the material being covered.[31]

Figure 4-5 summarizes the steps of the Development phase.

---

[31] This knowledgeable person could be a member of the organization's information security staff. A senior member of the same "community" as the target audience might be a good person to review material developed at the beginning or intermediate level. Having several people review course/module material can provide more beneficial feedback.

```
┌─────────────────────────────────────────────────────┐
│        List Activities Required for Each Objective    │
└─────────────────────────────────────────────────────┘
                          │
                          ▼
┌─────────────────────────────────────────────────────┐
│          Select Appropriate Delivery Method(s)        │
└─────────────────────────────────────────────────────┘
                          │
                          ▼
┌─────────────────────────────────────────────────────┐
│               Gather Reference Material               │
└─────────────────────────────────────────────────────┘
                          │
                          ▼
┌─────────────────────────────────────────────────────┐
│            Review Existing Course Material            │
└─────────────────────────────────────────────────────┘
                          │
                          ▼
┌─────────────────────────────────────────────────────┐
│               Develop Course Material                 │
└─────────────────────────────────────────────────────┘
                          │
                          ▼
┌─────────────────────────────────────────────────────┐
│        Develop Lesson Plans and Instructor Guide      │
└─────────────────────────────────────────────────────┘
                          │
                          ▼
┌─────────────────────────────────────────────────────┐
│            Expert Review of Course Materials          │
└─────────────────────────────────────────────────────┘
```
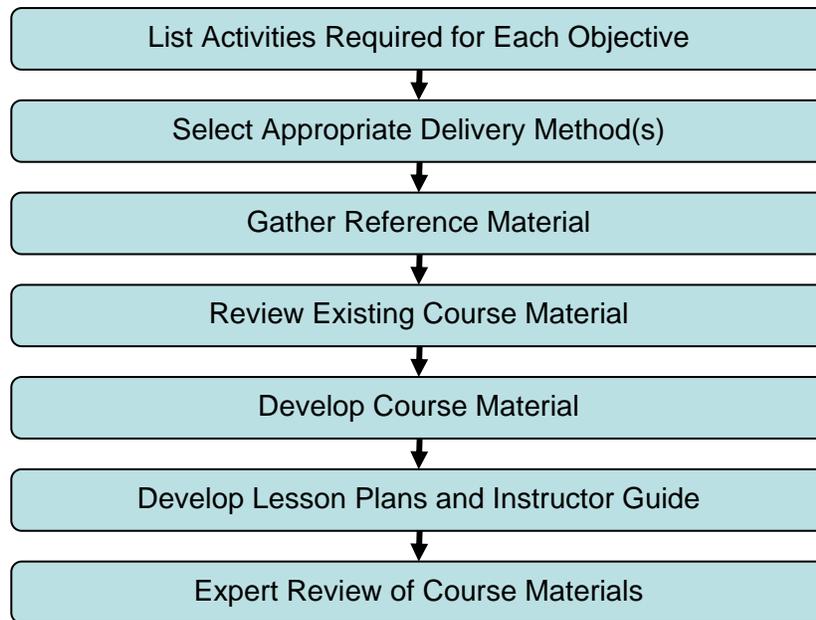
Figure 4-5: Development Phase

The outputs of the Development phase include a draft course or module with lesson plans and an instructor guide.

4.5.4.   Implementation

The draft course or module should be piloted to a hand-picked audience that can provide feedback on the material being presented and on the presentation methods. This pilot complements the expert review and allows the IDS or instructional design team to make any needed adjustments prior to full-scale production and delivery of the training. If "train the trainer" training is required, this can be accomplished after any adjustments are made following the pilot delivery. The course or module should then be ready for full-scale delivery. Figure 4-6 summarizes the steps of the Implementation phase.

```
┌─────────────────────────────────────────────────┐
│        Pilot Course to Hand-Picked Audience       │
└─────────────────────────────────────────────────┘
                        │
                        ▼
┌─────────────────────────────────────────────────┐
│              Make Course Adjustments              │
└─────────────────────────────────────────────────┘
                        │
                        ▼
┌─────────────────────────────────────────────────┐
│            Train the Trainer (if required)        │
└─────────────────────────────────────────────────┘
                        │
                        ▼
┌─────────────────────────────────────────────────┐
│                Full-Scale Delivery                │
└─────────────────────────────────────────────────┘
```
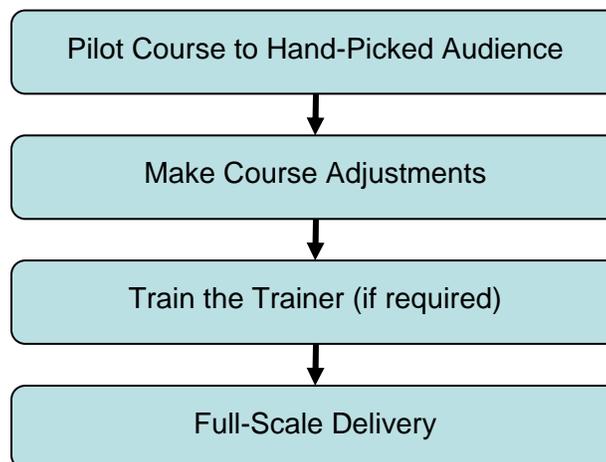
Figure 4-6: Implementation Phase

4.5.5.   Evaluation

This phase consists of two types of evaluation: 1) formative evaluation, and 2) summative evaluation.

- Formative evaluation is a method of judging the worth of a program while the program activities are forming or happening. Formative evaluation focuses on the *process*. Formative evaluation is present in each phase of the ADDIE process in the form of the continuous review of each assumption and each step of every phase. It is critical for the formative evaluation that the security professionals responsible for the training being developed remain in close contact with the IDS (or the instructional design team) responsible for developing the training. Formative evaluation answers the question: "Are we teaching what we are supposed to be teaching?"

- Summative evaluation is a method of judging the worth of the program at the end of program activities. Summative evaluation focuses on the *outcome*. Summative evaluation provides the opportunity for the students and their supervisors to provide feedback to the instructors and the instructional design team on whether the training is meeting the needs of the organization. Summative evaluation is typically conducted on four levels:

  o Level 1 – End-of-course evaluations that attempt to measure student satisfaction. This approach asks the question "Was this training effective for me?"

  o Level 2 – Behavioral objective testing of learning effectiveness, which is also a measure of teaching effectiveness.

  o Level 3 – Supervisor feedback on performance effectiveness which is completed six weeks to six months after the training. This approach asks the question, "Did the training make your employee more effective in their job?"

  o Level 4 – Organizational feedback which is typically completed on a cyclic basis. This approach asks the questions, "Is our training program delivering quality courses and the right mix of courses?"

Both forms of evaluation are needed for an effective and efficient role-based training program. More details on program evaluation and sample evaluation forms are provided in Appendix C.

Figure 4-7 summarizes the Evaluation phase.
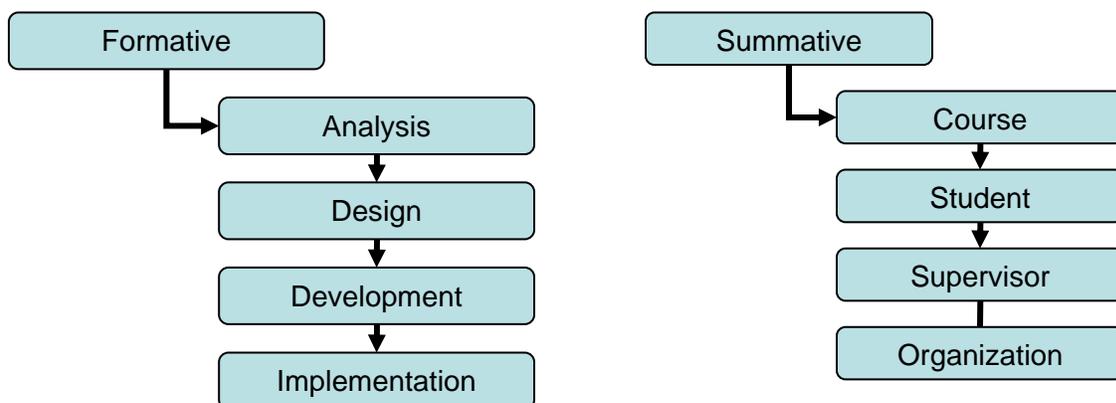
Figure 4-7: Evaluation Phase

4.6. A Worked Example of the ADDIE Process: Role-playing with Role-based Training

The organization has conducted a needs assessment of its information security training program. The assessment has identified a lack of training for the Information System Security Officers (ISSOs) as a gap in the current security training offerings. After checking current commercial offerings and government training sites for appropriate courses, the decision is made to develop an ISSO course specific to the organization.

4.6.1. The Analysis Phase

Figure 4-8 lists the steps to be performed in the Analysis phase.

1 - Select Tasks to Train
2 - Determine Knowledge Level Required
3 - Develop Behavioral Outcomes
4 - Develop Performance Measures
5 - Determine Prerequisite Knowledge
6 - Compare with Other Training Required
7 - Determine Appropriate Instructional Setting
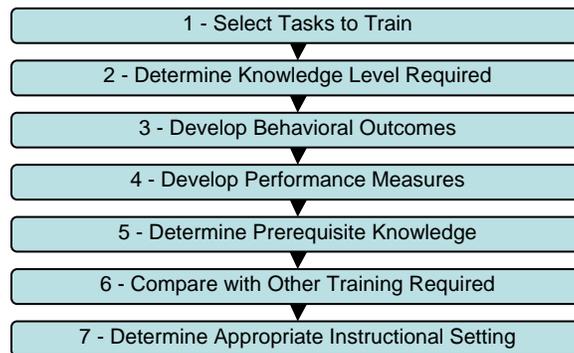
Figure 4-8: Analysis Phase

The organization uses an assignment letter process for designating ISSO's that lists 17 tasks (or responsibilities) of the ISSO. These 17 tasks will be the basis of the ISSO training.

(Step 1) One task or responsibility is as follows:

ISSO's are responsible for enforcing information security policies, standards and procedures on the system for which the ISSO is responsible.

- The IDS and the information security SME have determined that the ISSOs should have an advanced level of knowledge about applicable laws, regulations, and standards.[32]

- Referring to the role-specific matrix for ISSO's in Appendix A (Page A-7), the IDS and SME note that all five cells related to the training area Laws and Regulations (i.e., 1A, 1B, 1C, 1D, 1E) are selected for their consideration. They determine that in their organization's environment, it is prudent to present some information about laws and regulations as they impact each of the five responsibilities shown in the matrix since the target audience will likely have such responsibilities.

- Referring next to the cell description pages in Appendix B that describe how each cell or module should be built, the team notes that Pages B-2 and B-3 describe Cell 1A, Pages B-4 and B-5 describe Cell 1B, Pages B-6 and B-7 describe Cell 1C, Pages B-8 and B-9 describe Cell 1D, and Pages B-10 and B-11 describe Cell 1E. The cell description pages also show the recommended topic areas from the Information Security Training Topics and Elements (Exhibit 4-4) and the recommended additional resource documents.

---

[32] A training course or module may have a mix of beginning, intermediate, and advanced material, depending on the needs of the target audience.

- Referring to Exhibit 4-4 (Pages 32-37), the team reviews each of the recommended topics and their related elements. Based on their review of the needs assessment and on the job task analysis conducted on the ISSO population, the team fine-tunes the selection of topics and does the same for each topic's elements.[33] (Step 2)

(There are more tasks for people in this role; this worked example focuses on one.)

The cell description pages (Pages B-2 and B-3) in Appendix B for Cell 1A (Training Area = Laws and Regulations, Responsibility = Manage) contain terminal and enabling learning objectives that can be used to determine the expected behavioral outcome and any performance measure(s) that may be required to determine achievement. (Steps 3 and 4)

(There are more cells and cell description pages to be used in developing training material for this role; this worked example focuses on one cell and its corresponding cell description pages.)

Since this is an advanced level course, required prerequisite knowledge can be determined from the learning objectives contained in the cell description pages in Appendix B. If this prerequisite knowledge does not exist in other courses or training within the organization, consideration should be given to including these beginning and intermediate learning objectives as enabling objectives in the current course or module development. (Step 5)

An analysis of the additional roles that may require this same knowledge (by reviewing the cell description pages in Appendix B) will reveal how this cell or module can be used in other role-based training course development. In this case Senior Agency Information Security Officers, Chief Information Officers, Senior Information Resource Management Officials, Information Resource Managers, and Office of General Counsel Staff may also require this same level of knowledge.[34] (Step 6)

Given the material to be covered, the knowledge level required, and the number of people to be trained, an appropriate instructional setting can be selected. While no hard and fast rules exist, small numbers of training recipients and in-depth knowledge requirements tend to lend themselves to face-to-face in-class training and large numbers and less complex topics to web- or computer-based training. The choice will ultimately depend on the organization's preferences. (Step 7)

The results of these seven steps lead directly to the Design phase.

4.6.2. The Design Phase

Figure 4-9 lists the steps to be performed in the Design phase.

---

[33] The Analysis phase can include a job task analysis, although that may not be necessary. In some cases, a policy review will illuminate new material that needs to be added to an existing course. A review of existing training material by an SME can also identify gaps in that material.

[34] The instructional design team will determine whether a recommended cell is used in training courses or modules for the other roles shown at the bottom of each cell description page in Appendix B. The determination should be based on a review of the recommended cells for each role, and an understanding of what training is needed by prospective training recipients in those roles.
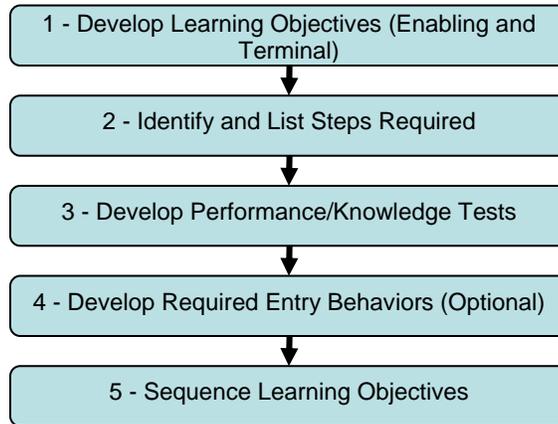
Figure 4-9: Design Phase

Using the learning objectives from the cell description pages in Appendix B and tailoring them to the organization's needs is the quickest way to develop enabling and terminal learning objectives. For example, the ISSO must "*know where to find federal government-wide and organization-specific published documents, such as laws, regulations, policies, guidelines, and standards*" (cell description page for Cell 1A, Appendix B, Pages B-2 and B-3) – ideal as an enabling objective supporting the terminal objective "*Analyze, approve, and issue policies (e.g., authorizes policies as part of an IRM manual)*". (Step 1)

In addition, using the key action words for each knowledge level listed in the cell description pages in Appendix B can assist in the development of learning objectives. (Note that for modules 1A, 2.1A, 2.2A, 3.1B, 3.2C, 3.3D, and 3.4E enabling learning objectives have been provided along with the terminal learning objectives. These are provided to demonstrate how enabling learning objectives are typically constructed.) Once the learning objectives are established, it is necessary to determine the actions required to accomplish each objective. (Step 2)

If testing will be required for this module, now is the time to develop the specific questions for this module. (Step 3)

This is also a good time to review the steps required for this objective to identify any prerequisite knowledge the student must have to take advantage of and fully benefit form the proposed steps to accomplish this objective. (Step 4)

Once enabling and terminal objectives - and the steps required to accomplish each - are developed for all of the ISSO tasks to be taught in this course (17 in the case of the ISSO), develop a logical sequence for presenting the objectives during the course. This may be as simple as sequencing them in the order listed in the assignment letter, but this step requires thought and discussion with current practitioners in the field. (Step 5)

Once the instructional sequence is decided, development of the course materials can begin.

4.6.3.   The Development Phase

Figure 4-10 lists the steps to be performed in the Development phase.

| 1 - List Activities Required for Each Objective |
| 2 - Select Appropriate Delivery Method |
| 3 - Gather Reference Material |
| 4 - Review Existing Course Material |
| 5 - Develop Course Material |
| 6 - Develop Lesson Plans and Instructor Guide |
| 7 - Expert Review of Course Materials |
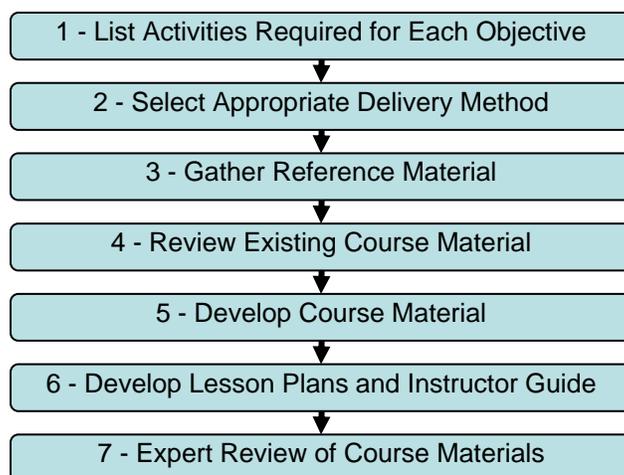
Figure 4-10: Development Phase

It is evident from these steps that the amount of quality time spent in the Analysis and Design phases will pay big dividends in course development. Reviewing the steps required to accomplish each objective will uncover activities that can assist in the accomplishment of the objective. (Step 1)

The appropriate instructional setting was determined during the Analysis phase and is now confirmed or modified. The instructional design team may determine that some material is suitable for technology-based delivery (e.g., web or computer) and other requires classroom interaction. In this step this decision should be made or confirmed. (Step 2)

Exhibit 4-4 (Pages 32-37) and Appendix B provide topics and elements. Appendix B also provides a list of publications in each cell description page that can be used to further develop topics and elements chosen to develop the course or module. Department, agency, and more local documents that contain policy and procedures pertaining to training areas in the course should also be collected. (Step 3)

After reviewing existing course material that may contain reusable information, development of course material can begin. (Steps 4 and 5)

Once the course material is developed, work can begin on lesson plans and the instructor guide while the material is being reviewed by current practitioners in the field. (Steps 6 and 7)

4.6.4. The Implementation Phase

Figure 4-11 lists the steps to be performed in the Implementation phase.

```
┌─────────────────────────────────┐
│  1 - Pilot Course to Hand-Picked │
│            Audience              │
└─────────────────────────────────┘
                │
                ▼
┌─────────────────────────────────┐
│     2 - Make Course Adjustments  │
└─────────────────────────────────┘
                │
                ▼
┌─────────────────────────────────┐
│   3 - Train the Trainer (if required) │
└─────────────────────────────────┘
                │
                ▼
┌─────────────────────────────────┐
│       4 - Full-Scale Delivery    │
└─────────────────────────────────┘
```
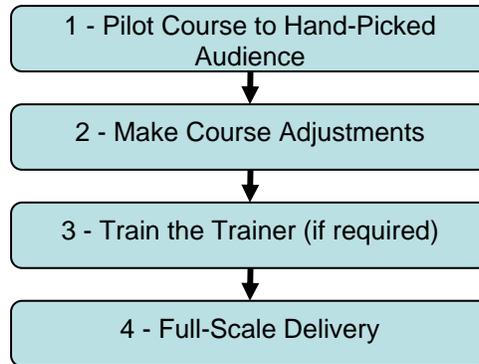
Figure 4-11: Implementation Phase

The importance of conducting a pilot course cannot be overstated. In this example of a course or module being built for ISSOs, the input of senior ISSOs, their managers, and training professionals – key parts of the "hand-picked" audience -provide valuable input in determining the success or failure of the course when given to its first "real" audience. (Steps 1 and 2)

"Train the trainer" training, if required, is typically accomplished with every attendee using the instructor's guide and focuses more on instructional delivery rather than content. (Step 3)

At this point the course is ready for full-scale delivery but the development process does not stop. (Step 4)

4.6.5.   The Evaluation Phase

Figure 4-12 summarizes the Evaluation phase.

```
┌──────────────┐               ┌──────────────┐
│  Formative   │               │  Summative   │
└──────────────┘               └──────────────┘
        │                              │
        ▼                              ▼
   ┌──────────────┐             ┌──────────────┐
   │   Analysis   │             │    Course    │
   └──────────────┘             └──────────────┘
        │                              │
        ▼                              ▼
   ┌──────────────┐             ┌──────────────┐
   │    Design    │             │   Student    │
   └──────────────┘             └──────────────┘
        │                              │
        ▼                              ▼
   ┌──────────────┐             ┌──────────────┐
   │ Development  │             │  Supervisor  │
   └──────────────┘             └──────────────┘
        │                              │
        ▼                              ▼
   ┌──────────────┐             ┌──────────────┐
   │Implementation│             │ Organization │
   └──────────────┘             └──────────────┘
```
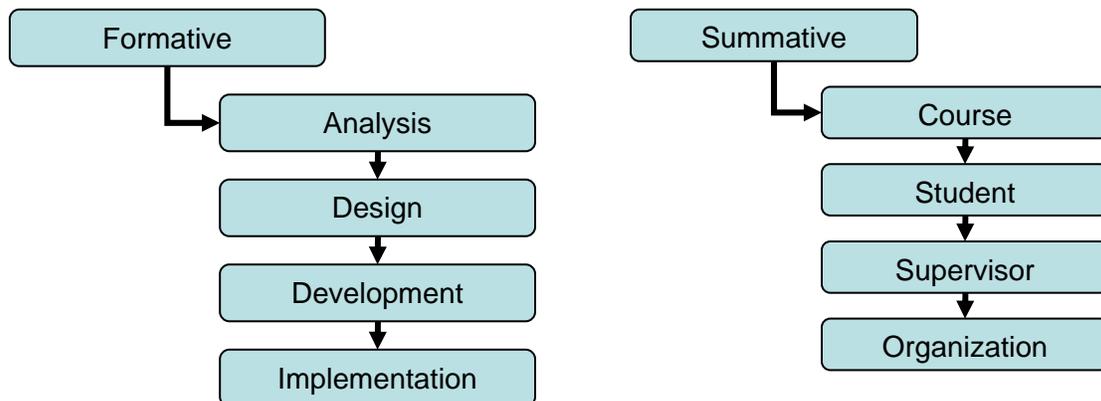
Figure 4-12: Evaluation Phase

During each phase of the ADDIE process, *formative evaluation* is concerned with the question: "Are we teaching what we're supposed to be teaching?" Other questions to ask include:

- Is there a better way to present a specific objective?

- Have the reference materials been updated?

- Have internal policies and procedures changes?

- Are there new senior managers responsible for the program?

Summative evaluation takes place at the conclusion of each course delivery and through out the year on a regular basis as determined by the organization. At each level of evaluation, a key question is asked, as indicated below:

- Level 1 – End-of-course evaluations that attempt to measure student satisfaction. This approach asks the question: "Was this training effective for me?" This is also the opportunity to collect information about the instructor's performance.

- Level 2 – Behavioral objective testing, completed at the end of the training, asks the question: "Did the student achieve the objectives of the training?" This approach also provides a measure of teaching effectiveness.

- Level 3 – Supervisor feedback, completed six weeks to six months after the training, asks the question: "Did the training make your employee more effective in the performance of their job?" This survey/questionnaire can also ask about training requirements the supervisor has that are not being met.

- Level 4 – Organizational feedback, typically completed on a cyclic basis, asks the questions: "Is our training program delivering quality courses and the right mix of courses?"

The goal of all evaluation is to improve the quality of the organization's information security training program, the quality of the instruction and the quality of the courses delivered. Accomplishing this enhances the information security posture of the organization.

More details on training program evaluation and sample evaluation forms are provided in Appendix C.

Appendix A: Role-Based Training Matrices

Introduction

Information security training is provided selectively, based on individual responsibilities and needs. Specifically, training is to be provided to individuals based on their particular role. Over time, individuals acquire different roles relative to information security within an organization, or as they make a career move to a different organization. Sometimes they will be users of 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 IT systems. An individual's need for information security training changes as their roles change. This is recognized within the Learning Continuum (see Page 12) by segmenting the Role-Based Training level into five responsibilities which represent categories of generic organizational responsibilities: Manage, Acquire, Design and Develop, Implement and Operate, and Review and Evaluate.

Role Matrices

This appendix contains role-specific matrices which include selected cells for each role that was listed in Exhibit 4-1 (Page 23). The cells shown in each matrix are recommendations, and are offered as a starting point for an organization's consideration. The mix of cells may require revision based on the organization's analysis of their specific needs.

Role: Agency Head / Other Executives					
	Responsibilities				
Training Areas	**A Manage**	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Assessor					
	Responsibilities				
Training Areas	**A Manage**	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Auditor, External					
	Responsibilities				
Training Areas	**A Manage**	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Auditor, Internal

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Authorizing Official

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Chief Information Officer (CIO)

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Contracting Officer

Training Areas	Responsibilities				
	A **Manage**	**B** **Acquire**	**C** **Design & Develop**	**D** **Implement & Operate**	**E** **Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Contracting Officer's Technical Representative (COTR)

Training Areas	Responsibilities				
	A **Manage**	**B** **Acquire**	**C** **Design & Develop**	**D** **Implement & Operate**	**E** **Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Data Center Manager

Training Areas	Responsibilities				
	A **Manage**	**B** **Acquire**	**C** **Design & Develop**	**D** **Implement & Operate**	**E** **Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Database Administrator

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C	███	3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A	███	███	3.5D	3.5E

Role: First Responders

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C	███	3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A	███	███	3.5D	3.5E

Role: Freedom of Information Act Official

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C	███	3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A	███	███	3.5D	3.5E

Role: Incident Response Coordinator

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Information Owner

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Information Resources Manager

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Information System Security Officer (ISSO)					
	Responsibilities				
Training Areas	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Network Administrator					
	Responsibilities				
Training Areas	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Office of General Counsel Staff					
	Responsibilities				
Training Areas	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Privacy Act Official					
	Responsibilities				
Training Areas	**A Manage**	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Program and Functional Managers					
	Responsibilities				
Training Areas	**A Manage**	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Programmer / Systems Analyst					
	Responsibilities				
Training Areas	**A Manage**	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Risk Executive

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Risk / Vulnerability Analyst

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Security Administrator

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Security Engineer

Training Areas	Responsibilities				
	A Manage	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C	■	3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A	■		3.5D	3.5E

Role: Senior Agency Information Security Officer (Information Security Officer / Manager)

Training Areas	Responsibilities				
	A Manage	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C	■	3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A	■		3.5D	3.5E

Role: Senior Information Resources Management Official

Training Areas	Responsibilities				
	A Manage	**B Acquire**	**C Design & Develop**	**D Implement & Operate**	**E Review &Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C	■	3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A	■		3.5D	3.5E

Role: Source Selection Board Member

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: System Administrator

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: System Designer/Developer

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: System Operations Personnel

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: System Owner

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Technical Support Personnel

Training Areas	Responsibilities				
	A Manage	B Acquire	C Design & Develop	D Implement & Operate	E Review &Evaluate
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Role: Telecommunications Specialist					
	Responsibilities				
Training Areas	**A** **Manage**	**B** **Acquire**	**C** **Design &** **Develop**	**D** **Implement** **& Operate**	**E** **Review** **&Evaluate**
1. Laws & Regulations	1A	1B	1C	1D	1E
2. Security Program					
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E
3. System Life Cycle Security					
3.1 Initiation	3.1A	3.1B	3.1C		3.1E
3.2 Development/Acquisition	3.2A	3.2B	3.2C	3.2D	3.2E
3.3 Implementation/Assessment	3.3A	3.3B	3.3C	3.3D	3.3E
3.4 Operations/Maintenance	3.4A	3.4B	3.4C	3.4D	3.4E
3.5 Disposal	3.5A			3.5D	3.5E

Appendix B: Information Security Training Curriculum Modules

Introduction

This appendix contains training curriculum modules or cell description pages for each of the cells available for use in a training matrix.

Each cell in a matrix in Appendix A has a corresponding cell description module or cell description pages in this appendix. The cell description contains information that is critical for an IDS to know when building a course. Each cell description module identifies the applicable training area and responsibility (e.g., manage, acquire, design and develop). Each cell description module also includes:

- the definition of the function of the cell as the intersection of a responsibility column and a training area row,

- the behavioral outcome that the material built for that cell should produce in the training recipient,

- knowledge levels (i.e., beginning, intermediate, advanced),

- terminal learning objectives for each of the three possible knowledge levels,[35] and

- specific information security-related topics from the Information Security Training Topics and Elements (Exhibit 4-4) that apply to that cell.

With the information contained in each cell description module or sheet, the IDS can begin to build training material that will make up the role-based training course or module.

---

[35] Terminal learning objectives are given for all cells in this appendix. In addition, enabling learning objectives are given for select cells, including Cells 1A, 2.1A, 2.2A, 3.1B, 3.2C, 3.3D, and 3.4E. These are provided to demonstrate how enabling learning objectives are typically constructed.

INFORMATION SECURITY TRAINING
Curriculum Module
Laws and Regulations (1A)

Training Area: **Federal/Departmental/Agency**
Responsibility: **Manage**

Definition — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources.

Behavioral Outcome — Managers are able to understand applicable governing documents and their interrelationships and interpret and apply them to the manager's area of responsibility.

Knowledge Levels —

1. Beginning — Research, Know, Identify
2. Intermediate — Analyze, Understand, Apply
3. Advanced — Interpret, Approve, Decide, Issue

Terminal and Enabling Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Know where to find federal government-wide and organization-specific published documents, such as laws, regulations, policies, guidelines, and standards and how to apply them.
   - Research – information security laws, regulations, policies, guidelines, and standards for applicability to the manager's area of responsibility.
   - Know – how and when information security laws, regulations, policies, guidelines, and standards affect daily procedures and processes; Agency and departmental missions; and employees within the manager's area of responsibility.
   - Identify – potential gaps and violations between department/agency policies, mandated requirements, and standards compared to daily procedures.
2. Intermediate — Develop policies that reflect the legislative intent of applicable laws and regulations (e.g., policies addressing software copyright law infringement).
   - Analyze – the impact of applicable information security laws and regulations to the manager's area of responsibility.
   - Understand – how applicable laws and regulations affect the manager's area of responsibility and interact with organizational goals and existing policy.

- Apply – mandated requirements and standards in the form of appropriate policies to the manager's area of responsibility.

3. Advanced — Analyze, approve, and issue policies (e.g., authorizes policies as part of an IRM manual).
- Interpret – whether policies have sufficiently covered mandated laws and regulations.
- Approve – policies as appropriate to the manager's area of responsibility.
- Decide - what action is required in reference to the law/policies.
- Issue – guidance on policies and promote policies to the manager's area of responsibility.

Applicable Roles (minimum) —

Chief Information Officer (CIO)	Information Resources Manager
Information Resources Management (IRM) Official, Senior	
Senior Agency Information Security Officer/Manager and Staff	
Information System Security Officer	Office of the General Counsel Staff

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
2. Information Security Program
7. Risk Management

RESOURCE DOCUMENTS

NIST SP 800-60v2 Appendix
FIPS 199
FIPS 200
NIST SP 800-53
NIST SP 800-64
NIST SP 800-18
NIST SP 800-30
NIST SP 800-37
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Laws & Regulations (1B)

Training Area: **Federal/Departmental/Agency**
Responsibility: **Acquire**

Definition — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources

Behavioral Outcome — Individuals involved in the acquisition of information technology resources have a sufficient understanding of information security requirements and issues to protect the government's interest in such acquisitions.

Knowledge Levels — (keywords)

1. Beginning — Identify, Know, Research
2. Intermediate — Analyze, Interpret, Develop, Decide
3. Advanced — Evaluate, Approve, Issue

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Identify security requirements to be included in statements of work and other appropriate procurement documents (e.g., procurement requests, purchase orders, task orders, and proposal evaluation summaries) as required by the federal regulations.

2. Intermediate — Develop security requirements specific to an information technology acquisition for inclusion in procurement documents (e.g., ensures that required controls are adequate and appropriate) as required by the federal regulations.

3. Advanced — Evaluate proposals to determine if proposed security solutions effectively address agency requirements as detailed in solicitation documents and are in compliance with federal regulations.

Applicable Roles (minimum) —

Contracting Officer	Source Selection Board Member
Contracting Officer's Technical Representative (COTR)	
Information Resources Management (IRM) Official, Senior	
Senior Agency Information Security Officer/Manager and Staff	
Information System Security Officer (ISSO)	Security Engineer

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
3. System Environment
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-36
NIST SP 800-35
NIST SP 800-23
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Laws & Regulations (1C)

Training Area: **Federal/Departmental/Agency**
Responsibility: **Design & Develop**

Definition — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources

Behavioral Outcome — Individuals responsible for the design and development of automated information systems are able to translate IT laws and regulations into technical specifications which provide adequate and appropriate levels of protection.

Knowledge Levels —

1. Beginning — Identify, Know, Apply
2. Intermediate — Research, Interpret, Develop
3. Advanced — Evaluate, Approve, Select

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Identify laws and regulations relevant to the specific system being designed (e.g., a financial management system would be subject to the requirements of the Accounting and Auditing Act, whereas a personnel system would be subject to the requirements of the Privacy Act).

2. Intermediate — Interpret applicable laws and regulations to develop security functional requirements (e.g., requiring encryption for Privacy Act data stored on a shared file server)

3. Advanced — Evaluate conflicting functional requirements (e.g., the level of audit trail that can be incorporated without adversely affecting system performance) and select for implementation those requirements that will provide the highest level of security at the minimum cost consistent with applicable laws and regulations.

Applicable Roles (minimum) —

Auditor, Internal	Information Resources Manager
Senior Agency Information Security Officer/Manager and Staff	
Program and Functional Managers	Programmer/Systems Analyst
System Designer/Developer	Information System Security Officer
Assessor	Security Engineer

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-53
NIST SP 800-64

INFORMATION SECURITY TRAINING
Curriculum Module
Laws & Regulations (1D)

Training Area: **Federal/Departmental/Agency**
Responsibility: **Implement & Operate**

Definition — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources.

Behavioral Outcome — Individuals responsible for the technical implementation and daily operations of an automated information system are able to understand information security laws and regulations in sufficient detail to ensure that appropriate safeguards are in place and enforced.

Knowledge Levels —

1. Beginning — Know, Identify, Apply
2. Intermediate — Investigate, Interpret, Decide, Analyze
3. Advanced — Evaluate, Decide, Approve

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Recognize a potential security violation and take appropriate action to report the incident as required by federal regulation and mitigate any adverse impact (e.g., block access to a communications port which has been subject to multiple invalid log-on attempts during non-duty hours).

2. Intermediate — Investigate a potential security violation to determine if the organization's policy has been breached and assess the impact of the breach (e.g., review audit trails to determine if inappropriate access has occurred).

3. Advanced — Determine whether a security breach is indicative of a violation of law that requires specific legal action (e.g., unauthorized access and alteration of data) and forward evidence to the Federal Bureau of Investigation for investigation.

Applicable Roles (minimum) ⎯

Senior Agency Information Security Officer/Manager and Staff	
Programmer/Systems Analyst	System Administrator
Systems Operations Personnel	Technical Support Personnel
Network Administrator	Security Administrator
Information System Security Officer	First Responders
Incident Response Coordinator	

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
7. Risk Management
8. Management Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-83
NIST SP 800-86
NIST SP 800-61
NIST SP 800-53

INFORMATION SECURITY TRAINING
Curriculum Module
Laws & Regulations (1E)

Training Area: **Federal/Departmental/Agency**
Responsibility: **Review & Evaluate**

Definition — Federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) governing mandated requirements and standards for the management and protection of information technology resources.

Behavioral Outcome — Individuals responsible for the review/evaluation of an automated information system are able to use information security laws and regulations in developing a comparative baseline and determining the level of system compliance.

Knowledge Levels — (keywords)

1. Beginning — Identify, Know, Apply
2. Intermediate — Develop, Interpret, Understand
3. Advanced — Evaluate, Decide, Approve

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Identify laws and regulations applicable to a specific information system or application (e.g., a payroll application is subject to OMB Circulars A-123, A-127, and A-130, while a project management system may only be subject to OMB Circular A-130).

2. Intermediate — Use laws, regulations, and agency guidance to develop a comparative information security requirements baseline appropriate to evaluate the existing security environment.

3. Advanced — Evaluate in-place controls and countermeasures against the comparative baseline to determine if the controls provide a security environment equal to or better than the baseline environment.

Applicable Roles (minimum) —

Auditor, External	Auditor, Internal	Certification Reviewer
Information Resources Manager		Information Systems Security Officer
Senior Agency Information Security Officer/Manager and Staff		

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-53A

Training Area: Information Security Program

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.1A)

Training Area: **Planning**
Responsibility: **Manage**

Definition — The design and establishment of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals involved in the management of information security programs are able to understand principles and processes of program planning and can organize resources to develop a security program that meets organizational needs.

Knowledge Levels —

1. Beginning — Participate, Know, Apply
2. Intermediate — Interpret, Develop, Decide
3. Advanced — Evaluate, Approve, Direct

Terminal and Enabling Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in the development or modification of the organization's information security program plans and requirements.
   - Participate – in the development or modification of the organization's information security program plans and requirements.
   - Know – information security fundamentals that should be included in program plans.
   - Apply – department/agency policies and associated SOP's as applicable to your program plan.

2. Intermediate — Develop and/or modify information security program policy, guidelines, and procedures and recommend associated resource allocations.
   - Interpret – regulations, guidelines and best practices for application in your information security program.
   - Develop – program policy, procedures, and guidelines to cover any gaps in existing documentation.

- Decide – on recommendations for associated resource allocations.

3. Advanced — Identify information security program implications of new technologies or technology upgrades. Review and approve various information security plans for appropriateness and effectiveness. Set priorities for allocation of resources.

- Evaluate – new technologies as they are developed for their information security implications and applications.
- Approve – information security plans created by programs and projects for their compliance with existing policies and procedures.
- Direct – funding to cover gaps in coverage of information security controls.

Applicable Roles (minimum) —

Information Resources Manager	Program and Functional Managers	
Senior Agency Information Security Officer/Manager and Staff		
Information Owner	Chief Information Officer	System Owner
Information System Security Officer		

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objective
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-14
NIST SP 800-27
NIST SP 800-33
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.1B)

Training Area: **Planning**
Responsibility: **Acquire**

Definition — The design and establishment of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals involved in planning the information security program can identify the resources required for successful implementation. Individuals recognize the need to include information security requirements in IT acquisitions and to incorporate appropriate acquisition policy and oversight in the information security program.

Knowledge Levels —

1. Beginning/Intermediate — Develop, Interpret, Decide, Apply
2. Advanced — Evaluate, Interpret, Approve, Issue

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate — Develop security requirements for hardware, software, and services acquisitions specific to the information security program (e.g., purchase of virus-scanning software or security reviews) and for inclusion in general IT acquisition guidance.

2. Advanced — Interpret and/or approve security requirements relative to the capabilities of new information technologies, revise IT acquisition guidance as appropriate, and issue changes.

Applicable Roles (minimum) —

Contracting Officer	Information Resources Manager
Contracting Officer's Technical Representative (COTR)	
Senior Agency Information Security Officer/Manager and Staff	
Source Selection Board Member	Telecommunications Specialist
Source Selection Board Member	Information System Security Officer

INFORMATION SECURITY TRAINING TOPICS

2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-14
NIST SP 800-27
NIST SP 800-33
NIST SP 800-36
NIST SP 800-35
NIST SP 800-23
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.1C)

Training Area: **Planning**
Responsibility: **Design & Develop**

Definition — The design and establishment of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals responsible for the design and development of an information security program are able to create a security program plan specific to a business process or organizational entity.

Knowledge Levels —

1. Beginning — Locate, Understand, Apply
2. Intermediate/Advanced — Design, Develop, Decide

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Understand the various components of an effective information security program and relate them to the organization's business process requirements.

2. Intermediate/Advanced — Design, develop, or modify information security program requirements.

Applicable Roles (minimum) —

Chief Information Officer (CIO)	Information Resources Manager
Senior Information Resources Management Official	
Senior Agency Information Security Officer/Manager and Staff	
Information System Security Officer (ISSO)	Incident Response Coordinator

INFORMATION SECURITY TRAINING TOPICS

2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-14
NIST SP 800-27
NIST SP 800-33
NIST SP 800-53
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.1D)

Training Area: **Planning**
Responsibility: **Implement & Operate**

Definition — The design and establishment of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals responsible for implementing and operating an information security program are able to develop plans for security controls, countermeasures, and processes as required to execute the existing program.

Knowledge Levels —

1. Beginning — Understand, Participate, Develop, Apply
2. Intermediate/Advanced — Approve, Allocate, Interpret, Direct

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in the development of plans for implementing information security program elements (e.g., develop procedures for screening new employees).

2. Intermediate/Advanced — Develop implementation strategies and resource estimates required to achieve information security goals. Allocate resources among competing tasks to achieve the maximum level of security at optimum cost.

Applicable Roles (minimum) —

Auditor, Internal	Chief Information Officer (CIO)
Senior Information Resources Management Official	
Senior Agency Information Security Officer/Manager and Staff	
Information Resources Manager	Information System Security Officer
System Administrator	Network Administrator
Security Administrator	Assessor
Incident Response Coordinator	

INFORMATION SECURITY TRAINING TOPICS

2. Information Security Program
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-14
NIST SP 800-27
NIST SP 800-33
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.1E)

Training Area: **Planning**
Responsibility: **Review & Evaluate**

Definition — The design and establishment of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals responsible for the review/evaluation of an information security program are able to review the program to determine its continuing capability to cost-effectively address identified requirements.

Knowledge Levels —

1. Beginning/Intermediate — Review, Know, Interpret
2. Advanced — Evaluate, Approve, Recommend

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate — Review the plans for implementing information security program elements to ensure that they effectively address program objectives.

2. Advanced — Provide recommendations for correcting identified deficiencies. Evaluate action plans for correcting identified deficiencies and provide recommendations for strengthening the information security program plans.

Applicable Roles (minimum) —

Auditor, External	Auditor, Internal	CIO
Senior Information Resources Management Official		
Senior Agency Information Security Officer/Manager and Staff		
Information System Security Officer	Office of the General Counsel Staff	
Assessor	Agency Head / Other Executives	
Risk Executive		

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-14
NIST SP 800-27
NIST SP 800-33
NIST SP 800-37
NIST SP 800-53A
NIST SP 800-26
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.2A)

Training Area: **Management**
Responsibility: **Manage**

Definition — The implementation and use of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals involved in information security program management understand and are able to implement a security program that meets their organization's needs

Knowledge Levels —

1. Beginning — Recognize, Know, Apply
2. Intermediate — Evaluate, Know, Review
3. Advanced — Determine, Interpret, Direct

Terminal and Enabling Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Monitor organizational activities to ensure compliance with the existing information security program (e.g., ensure that all IT systems have been identified and security plans prepared).
   - Recognize - when and where your programs do not comply with the agency information security program.
   - Know – the authorization status of all IT systems and their security plans.
   - Apply – procedures to integrate information security into the strategic planning, capital planning, and investment processes.

2. Intermediate — Review organizational information security plans to ensure that they appropriately address the security requirements of each system.
   - Evaluate – level of compliance of security plans, the status of any plan of action and milestones, and their overall residual risk level to the organization.
   - Know – the requirements and their affect on the interactions of different security controls at different levels.
   - Review – security plans at least annually.

3. Advanced — Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the information security program and, on that basis, modify or augment the program as appropriate.

- Determine - where deficiencies in the overall security program lie.
- Interpret – the deficiencies and their effect on the security program.
- Direct – resources to cover the deficiencies in a cost effective manner.

Applicable Roles (minimum) —

Chief Information Officer (CIO)	Information Resources Manager
Senior Agency Information Security Officer/Manager and Staff	
Program and Functional Managers	Information System Security Officer

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.2B)

Training Area: **Management**
Responsibility: **Acquire**

Definition — The implementation and use of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation

Behavioral Outcome — Individuals involved in managing the information security program have a sufficient understanding of information security and the acquisition process to incorporate information security program requirements into acquisition work steps.

Knowledge Levels —

1. Beginning — Identify, Know, Apply
2. Intermediate — Define, Develop, Write
3. Advanced — Evaluate, Determine, Approve

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Identify areas within the acquisition process where information security work steps are required.

2. Intermediate — Develop security work steps for inclusion in the acquisition process, e.g., requiring an information security officer review of statements of work.

3. Advanced — Evaluate procurement activities to ensure that information security work steps are being effectively performed.

Applicable Roles (minimum) —

Contracting Officer	Information Resources Manager
Contracting Officer's Technical Representative (COTR)	
Senior Agency Information Security Officer/Manager and Staff	
Source Selection Board Member	Information System Security Officer

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
2. Information Security Program
3. System Environment
9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-36
NIST SP 800-35
NIST SP 800-23
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.2C)

Training Area: **Management**
Responsibility: **Design & Develop**

Definition — The implementation and use of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals responsible for the design and development of an information security program have sufficient understanding of the appropriate program elements and requirements to be able to translate them into detailed policies and procedures which provide adequate and appropriate protection for the organization's IT resources in relation to acceptable levels of risk.

Knowledge Levels —

1. Beginning — Know, Research, Understand
2. Intermediate — Interpret, Decide, Establish, Apply
3. Advanced — Analyze, Interpret, Approve, Direct

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Understand categories of risk and participate in the design and development of operational information security program procedures.

2. Intermediate — Establish acceptable levels of risk and translate the information security program elements into operational procedures for providing adequate and appropriate protection of the organization's IT resources.

3. Advanced — Design, develop, and direct the activities necessary to marshal the organizational structures, processes, and people for an effective information security program implementation.

Applicable Roles (minimum) —

Chief Information Officer (CIO)	Information Resources Manager
Senior Information Resources Management Official	
Senior Agency Information Security Officer/Manager and Staff	
Information System Security Officer	

INFORMATION SECURITY TRAINING TOPICS

2. Information Security Program
7. Risk Management
9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP800-53
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.2D)

Training Area: **Management**
Responsibility: **Implement & Operate**

Definition — The implementation and use of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals who are responsible for the implementation and daily operations of an information security program have a sufficient understanding of the appropriate program elements and requirements to be able to apply them in a manner which provides adequate and appropriate levels of protection for the organization's IT resources.

Knowledge Levels —

1. Beginning — Identify, Understand, Apply
2. Intermediate — Interpret, Analyze, Decide
3. Advanced — Investigate, Approve, Direct

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Apply organization-specific information security program elements to the implementation of the program and identify areas of weakness.

2. Intermediate — Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risks.

3. Advanced — Direct the implementation of appropriate operational structures and processes to ensure an effective information security program.

Applicable Roles (minimum) —

Senior Information Resources Management Official		
Chief Information Officer	Program and Functional Managers	
System Administrator	Internal Auditor	System Owner
Information Resources Manager	Information System Security Officer	
Network Administrator	Security Administrator	
Senior Agency Information Security Officer/Manager and Staff		
Assessor	Incident Response Coordinator	

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
Security Management (2.2E)

Training Area: **Management**
Responsibility: **Review & Evaluate**

Definition — The implementation and use of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals responsible for the review/evaluation of an information security program have an adequate understanding of information security laws, regulations, standards, guidelines, and the organizational environment to determine if the program adequately addresses all threats and areas of potential vulnerability.

Knowledge Levels —

1. Beginning — Understand, Evaluate, Apply
2. Intermediate — Research, Compile, Interpret, Decide, Write
3. Advanced — Direct, Validate, Oversee

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in the review of an organization's information security program and evaluate the extent to the program is being managed effectively.

2. Intermediate — Develop compliance findings and recommendations.

3. Advanced — Direct the review of the management of an organization's information security program, validate findings and recommendations, and establish follow-up monitoring for corrective actions.

Applicable Roles (minimum) —

Auditor, External	Auditor, Internal	Chief Information Officer
Senior Information Resources Management Official		
Senior Information Security Officer/Manager and Staff		
Information System Security Officer		Office of General Counsel Staff
Agency Head / Other Executives	Assessor	Risk Executive

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-37
NIST SP 800-53A
NIST SP 800-26
NIST SP 800-100

Training Area: System Life Cycle Security

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.1A)

Training Area: **Initiation**
Responsibility: **Manage**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The initiation phase is the series of steps followed to ensure that security requirements are considered and resolved as new information systems and technologies are planned.

Behavioral Outcome — Individuals with management responsibilities are able to identify steps in the system development life cycle where security requirements and concerns (e.g., confidentiality, integrity, and availability) need to be considered and to define the processes to be used to resolve those concerns.

Knowledge Levels —

1. Beginning — Understand, Know, Recognize
2. Intermediate — Identify, Assess, Decide
3. Advanced — Analyze, Approve, Direct

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Understand the need to plan security into new information systems from the beginning and the benefits to be derived from doing so.

2. Intermediate — Identify alternative functional information security strategies to address system security concerns.

3. Advanced — Analyze identified information security strategies and select those that are the best approach/practice.

Applicable Roles (minimum) ⸺

Information Resources Manager		Program and Functional Managers	
Senior Agency Information Security Officer/Manager and Staff			
Information Owner	System Designer/Developer	System Owner	
Information System Security Officer			

INFORMATION SECURITY TRAINING TOPICS

2. Information Security Program
5. Information Sharing
6. Security Objectives
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-30
NIST SP 800-64
NIST SP 800-100

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The initiation phase is the series of steps followed to ensure that security requirements are considered and resolved as new information systems and technologies are planned.

Behavioral Outcome — Individuals with acquisition responsibilities are able to analyze and develop acquisition documents and/or provide guidance which ensures that functional information security requirements are incorporated.

Knowledge Levels —

1. Beginning — Identify, Locate, Understand
2. Intermediate — Develop, Research, Write
3. Advanced — Analyze, Evaluate, Approve

Terminal and Enabling Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Identify general and system-specific information security specifications which pertain to a particular system acquisition being planned.
- Identify – the general and system-specific information security specifications that pertain to the system acquisition being planned. (The plan should include: a needs determination, an initial definition of the system, a preliminary concept for the basic system, a preliminary definition of requirements, feasibility & technology assessments.)
- Locate - the security categorization using federal standards and guidelines and conduct a preliminary risk assessment for the planned information system so the results may be reviewed when in the decision-making process in the acquisition phase.
- Understand – the system security according to levels of impact (to confidentiality,

availability, and integrity) and select a baseline of initial security controls for those impact levels

2. Intermediate — Develop security-related portions of acquisition documents.
- Develop - an investment analysis to determine the appropriate strategy for achieving the system requirements, while taking mission needs and budget constraints into account. (Expenditures for security should be considered before the system is built because it is difficult to add functionality into a system after it has been built; it is usually more cost effective to include preventive security measures from the beginning.)
- Research – and conduct a thorough market analysis, alternative analysis and affordability assessment to determine the best solution for obtaining the needed capability. [Quantify the cost, schedule, performance, and benefit baselines for the solution(s).]
- Write - a requirements analysis commensurate with the size and complexity of the need that draws on and further develops the work performed.

3. Advanced — Ensure that security-related portions of the system acquisition documents meet all identified security needs.
- Analyze – suggested solutions.
- Evaluate – security-related portions of the system acquisition documents to ensure they meet all identified security needs.
- Approve – the security-related portions of the system acquisition documents.

Applicable Roles (minimum) —

Contracting Officer	System Designer/Developer	Information Owner
Contracting Officer's Technical Representative (COTR)		
Senior Agency Information Security Officer/Manager and Staff		
System Owner	Information System Security Officer	

INFORMATION SECURITY TRAINING TOPICS

2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS
NIST SP 800-18 NIST SP 800-23 NIST SP 800-30 NIST SP 800-35 NIST SP 800-36 NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.1C)

Training Area: **Initiation**
Responsibility: **Design & Develop**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The initiation phase is the series of steps followed to ensure that security requirements are considered and resolved as new information systems and technologies are planned.

Behavioral Outcome — Individuals responsible for the design and development of IT systems are able to translate information security requirements into system- level security specifications.

Knowledge Levels —

1. Beginning — Identify, Define, Participate
2. Intermediate — Understand, Interpret, Translate
3. Advanced — Analyze, Determine, Approve

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Identify areas where specific information security countermeasures are required and participate in the development of security strategies.

2. Intermediate — Translate information security strategies into initial security specifications for the planned system.

3. Advanced — Approve information security specifications for inclusion in the formal system baseline.

Applicable Roles (minimum) —

Senior Agency Information Security Officer/Manager and Staff		
Program and Functional Managers	Information System Security Officer	
System Designer/Developer	Information Owner	System Owner
Risk / Vulnerability Analyst		

INFORMATION SECURITY TRAINING TOPICS

2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-30
NIST SP 800-53
NIST SP 800-64
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.1E)

Training Area: **Initiation**
Responsibility: **Review & Evaluate**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The initiation phase is the series of steps followed to ensure that security requirements are considered and resolved as new information systems and technologies are planned.

Behavioral Outcome — Individuals are able to evaluate planning documents associated with a particular system to ensure that appropriate information security requirements have been considered and incorporated.

Knowledge Levels —

1. Beginning — Understand, Participate, Assess
2. Intermediate — Conduct, Research, Interpret
3. Advanced — Verify, Analyze, Recommend

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in the evaluation of functional information security requirements for a system.

2. Intermediate — Conduct the review and evaluation of functional information security requirements for a system.

3. Advanced — Verify that the security requirements for a system are appropriately incorporated into the system design.

Applicable Roles (minimum) —

Auditor, External	Auditor, Internal	Information Owner
System Owner		Information System Security Officer
Information Resources Manager		Office of General Counsel Staff
Senior Agency Information Security Officer/Manager and Staff		
Agency Head / Other Executives	Assessor	Risk Executive

INFORMATION SECURITY TRAINING TOPICS

2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-30
NIST SP 800-37
NIST SP 800-53A
NIST SP 800-26
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.2A)

Training Area: **Development/Acquisition**
Responsibility: **Manage**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The development/acquisition phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

Behavioral Outcome — Individuals with management responsibilities are able to ensure that the formal developmental baseline includes approved security requirements and that security-related features are installed, clearly identified, and documented.

Knowledge Levels —

1. Beginning — Understand, Know, Apply
2. Intermediate — Identify, Review, Decide
3. Advanced — Evaluate, Analyze, Approve

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Understand the relationship between planned security safeguards and the features being installed on the system under development. Provide input on security concerns during system development efforts.

2. Intermediate — Review the selected security safeguards to determine if security concerns identified in the approved plan have been fully addressed.

3. Advanced — Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed for the system being developed or modified.

Applicable Roles (minimum) —

Information Resources Manager		Information System Security Officer	
Senior Agency Information Security Officer/Manager and Staff			
System Designer/Developer	Information Owner		System Owner
Security Engineer			

INFORMATION SECURITY TRAINING TOPICS

4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-65
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.2B)

Training Area: **Development/Acquisition**
Responsibility: **Acquire**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The development/acquisition phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

Behavioral Outcome — Individuals with acquisition responsibilities are able to monitor procurement actions to ensure that information security requirements are satisfied.

Knowledge Levels —

1. Beginning — Identify, Know, Apply
2. Intermediate/Advanced — Evaluate, Analyze, Interpret

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Ensure that information security requirements are appropriately identified in acquisition documents.

2. Intermediate/Advanced — Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents.

Applicable Roles (minimum) —

Contracting Officer	Information System Security Officer
Contracting Officer's Technical Representative (COTR)	
Senior Agency Information Security Officer/Manager and Staff	
Source Selection Board Member	
System Owner	Authorizing Official
Security Engineer	

INFORMATION SECURITY TRAINING TOPICS

9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64
NIST SP 800-36
NIST SP 800-35
NIST SP 800-23
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.2C)

Training Area: **Development/Acquisition**
Responsibility: **Design & Develop**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The development/acquisition phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

Behavioral Outcome — Individuals responsible for system design, development or modification are able to use baseline information security requirements to select and install appropriate safeguards.

Knowledge Levels —

1. Beginning — Know, Construct, Apply
2. Intermediate — Identify, Recommend, Interpret
3. Advanced — Determine, Select, Approve

Terminal and Enabling Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in the construction of the IT system in accordance with the formal design specifications: developing manual procedures, using off-the-shelf hardware/software components, writing program code, customizing hardware components, and/or using other IT capabilities.
   - Know – the category of information that is on the system (low, moderate, high) so that you start with the proper baseline information security requirements. Find and apply the appropriate baseline for the system.
   - Construct – the IT system design specifications: developing manual procedures, using off-the-shelf hardware/software components, writing program code, customizing hardware components, and/or using other IT capabilities
   - Apply – the design and ensure that the appropriate safeguards are incorporated

into the system

2. Intermediate — Identify and recommend alternative safeguards that will satisfy baseline security specifications.
- Identify –alternative safeguards that will satisfy baseline security specifications.
- Recommend – alternative safeguards that will satisfy baseline security specifications.
- Interpret – whether or not alternative safeguards will better satisfy baseline security specifications and be more cost-effective

3. Advanced — Review recommendations and select appropriate safeguards for implementation.
- Determine – which safeguards will better satisfy baseline security specifications and are more cost-effective.
- Select – the most appropriate safeguards for implementation.
- Approve – appropriate safeguards for implementation.

Applicable Roles (minimum) —

Freedom of Information Act Official	Information System Security Officer
Senior Agency Information Security Officer/Manager and Staff	
System Designer/Developer	Privacy Act Official	Authorizing Official
Programmer/Systems Analyst	Risk / Vulnerability Analyst
Security Engineer	Assessor

INFORMATION SECURITY TRAINING TOPICS

2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-53
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.2D)

Training Area: **Development/Acquisition**
Responsibility: **Implement & Operate**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The development/acquisition phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

Behavioral Outcome — — Individuals responsible for system implementation or operation are able to assemble, integrate, and install systems so that the functionality and effectiveness of safeguards can be tested and evaluated.

Knowledge Levels —

1. Beginning — Install, Operate, Understand
2. Intermediate — Analyze, Approve, Recommend
3. Advanced — Direct, Require, Ensure

Terminal Learning Objectives —
At the conclusion of this module, individuals will be able to:

1. Beginning — Install and operate the IT systems in a test configuration in a manner that does not alter the program code or compromise security safeguards.

2. Intermediate — Analyze system performance for potential security problems (e.g., failure to update access control tables, corrupted data).

3. Advanced — Provide direction to system developers regarding correction of security problems identified during testing.

Applicable Roles (minimum) —

Data Center Manager	Network Administrator	Database Administrator
Security Administrator	System Administrator	System Designer/Developer
Senior Agency Information Security Officer/Manager and Staff		
System Operations Personnel	Technical Support Personnel	
Information System Security Officer	Security Engineer	

INFORMATION SECURITY TRAINING TOPICS

3. System Environment
4. System Interconnection
5. Information Sharing
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.2E)

Training Area: **Development/Acquisition**
Responsibility: **Review & Evaluate**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The development/acquisition phase is the series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

Behavioral Outcome — Individuals responsible for review and evaluation are able to examine development efforts at specified milestones to ensure that approved safeguards are in place and documented.

Knowledge Levels —

1. Beginning — Know, Review, Evaluate
2. Intermediate/Advanced — Analyze, Recommend, Approve

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Review IT system development documents for inclusion of appropriate safeguards.

2. Intermediate — Review and evaluate IT system development documents to ensure that system safeguards, as a whole, result in an acceptable level of risk.

3. Advanced — Evaluate configuration controls, review development of security test plans and procedures, and ensure that security requirements are documented and comply with the formal design specification.

Applicable Roles (minimum) ⎯

Auditor, External	Auditor, Internal	Certification Reviewer
Designated Approving Authority (DAA)		
Senior Agency Information Security Officer/Manager and Staff		
Program and Functional Managers	Information System Security Officer	
Information Owner	System Owner	
Office of General Counsel Staff	Assessor	Security Engineer
Risk Executive	Agency Head / Other Executives	

INFORMATION SECURITY TRAINING TOPICS

7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST 800-26
NIST 800-37
NIST 800-30
NIST 800-53
NIST 800-53A
NIST SP 800-100

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.3A)

Training Area: **Implementation/Assessment**
Responsibility: **Manage**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The implementation/assessment phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.

Behavioral Outcome — Individuals with management responsibilities are able to oversee the implementation and deployment of an IT system in a manner that does not compromise in-place and tested security safeguards.

Knowledge Levels —

1. Beginning/Intermediate/Advanced — Understand, Ensure, Decide

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate/Advanced — Decide whether to continue system deployment if unanticipated circumstances are encountered that compromise security safeguards. Ensure that final implementation in the production environment does not compromise security safeguards.

Applicable Roles (minimum) —

Senior Information Resources Management Official	
Information Resources Manager	Program and Functional Managers
Senior Agency Information Security Officer/Manager and Staff	
Information Owner	System Owner
Information System Security Officer	Security Engineer

INFORMATION SECURITY TRAINING TOPICS

3. System Environment
4. System Interconnection
5. Information Sharing
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-30
NIST SP 800-64
NIST SP 800-37
NIST SP 800-30

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.3B)

Training Area: **Implementation/Assessment**
Responsibility: **Acquire**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The implementation/assessment phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.

Behavioral Outcome — Individuals with acquisition responsibilities are able to ensure that the system, as implemented, meets all contractual requirements related to the security and privacy of IT resources.

Knowledge Levels —

1. Beginning/Intermediate — Know, Review, Decide
3. Advanced — Determine, Interpret, Authorize

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate — Monitor contract performance and review deliverables for conformance with contract requirements related to information security and privacy.

3. Advanced — Take action as needed to ensure that accepted products meet contract requirements.

Applicable Roles (minimum) —

Contracting Officer	Program and Functional Managers
Contracting Officer's Technical Representative (COTR)	
Senior Agency Information Security Officer/Manager and Staff	
Information Owner	System Owner
Information System Security Officer (ISSO)	Security Engineer

INFORMATION SECURITY TRAINING TOPICS

9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-30
NIST SP 800-64
NIST SP 800-37
NIST SP 800-30
NIST SP 800-36
NIST SP 800-35
NIST SP 800-23

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.3C)

Training Area: **Implementation/Assessment**
Responsibility: **Design & Develop**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The implementation/assessment phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.

Behavioral Outcome — Individuals responsible for system design and/or modification are able to participate in the development of procedures which ensure that safeguards are not compromised as they are incorporated into the production environment.

Knowledge Levels —

1. Beginning — Know, Understand, Identify
2. Intermediate — Interpret, Assess, Apply
3. Advanced — Determine, Recommend, Select

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Identify information security impacts associated with system implementation procedures.

2. Intermediate — Participate in the design, development, and modification of safeguards to correct vulnerabilities identified during system implementation.

3. Advanced — Lead the design, development, and modification of safeguards to correct vulnerabilities identified during system implementation.

Applicable Roles (minimum) —

Database Administrator	System Administrator	Security Administrator
Senior Agency Information Security Officer/Manager and Staff		
Network Administrator	System Designer/Developer	Authorizing Official
Program and Functional Managers	Programmer/Systems Analyst	
Systems Operations Personnel	Information System Security Officer	
Assessor	Security Engineer	Risk / Vulnerability Analyst

INFORMATION SECURITY TRAINING TOPICS

3. System Environment
4. System Interconnection
5. Information Sharing
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-30
NIST SP 800-64
NIST SP 800-37
NIST SP 800-30
NIST SP 800-53

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.3D)

Training Area: **Implementation/Assessment**
Responsibility: **Implement & Operate**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The implementation/assessment phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.

Behavioral Outcome — Individuals responsible for system implementation or operation ensure that approved safeguards are in place and effective as the system moves into production.

Knowledge Levels —

1. Beginning — Know, Apply, Recognize
2. Intermediate — Identify, Interpret, Decide
3. Advanced — Analyze, Determine, Approve

Terminal and Enabling Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in the implementation of safeguards for an IT system in accordance with the established implementation plan.
   - Know – how to implement safeguards for an IT system following an implementation plan.
   - Apply – security safeguards to an IT system in accordance with its implementation plan.
   - Recognize – whether or not safeguards are implemented (according to the implementation plan) and effective.

2. Intermediate — Identify vulnerabilities resulting from a departure from the implementation plan or that were not apparent during testing. Determine necessary

actions to return the implementation process to the established plan or to forward identified vulnerabilities for resolution.

- Identify – new vulnerabilities introduced by a departure from the implementation plan.
- Interpret – impact of the new vulnerabilities on the system.
- Decide – what action to take to resolve the new vulnerabilities

3. Advanced — Examine unresolved system vulnerabilities and determine what corrective action or additional safeguards are necessary to mitigate them.

- Analyze – whether to close, mitigate, watch or accept the vulnerability based on it's severity and available resources.
- Determine – if the cost of closing or mitigating the vulnerability is acceptable to the system and the funds available.
- Approve – the direction chosen for the final vulnerabilities.

Applicable Roles (minimum) —

Database Administrator	Network Administrator	System Administrator
Senior Agency Information Security Officer/Manager and Staff		
Security Administrator	Technical Support Personnel	First Responders
Systems Operations Personnel	Programmer/Systems Analyst	
Chief Information Officer	Data Center Manager	
Information System Security Officer	Security Engineer	
Risk / Vulnerability Analyst		

INFORMATION SECURITY TRAINING TOPICS

3. System Environment
4. System Interconnection
5. Information Sharing
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-30
NIST SP 800-64
NIST SP 800-37
NIST SP 800-30

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.3E)

Training Area: **Implementation/Assessment**
Responsibility: **Review & Evaluate**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The implementation/assessment phase is the installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.

Behavioral Outcome — Individuals responsible for review and evaluation are able to analyze system and test documentation to determine whether the system provides adequate and appropriate information security to support certification and accreditation.

Knowledge Levels —

1. Beginning/Intermediate — Understand, Review, Evaluate
3. Advanced — Analyze, Decide, Recommend

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate — Review and evaluate the effectiveness of safeguards, the maintainability of information security features, the adequacy of system documentation, and the efficiency of system security administration.

3. Advanced — Recommend IT system certification/accreditation and/or measures required to achieve/maintain approval to operate.

Applicable Roles (minimum) —

Auditor, External	Auditor, Internal	Information Owner
Senior Agency Information Security Officer/Manager and Staff		
Senior Information Resources Management Official		
Program and Functional Managers	Office of the General Counsel Staff	
Information System Security Officer	System Owner	
Agency Head / Other Executives	Risk Executive	
Assessor	Security Engineer	

INFORMATION SECURITY TRAINING TOPICS

3. System Environment
4. System Interconnection
6. Security Objectives
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-30
NIST SP 800-37
NIST SP 800-64

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.4A)

Training Area: **Operations/Maintenance**
Responsibility: **Manage**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The operations/maintenance phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

Behavioral Outcome — — Individuals with management responsibilities are able to monitor operations to ensure that safeguards are effective and have the intended effect of balancing efficiency with minimized risk.

Knowledge Levels —

1. Beginning — Know, Understand, Decide
2. Intermediate — Direct, Provide, Identify
3. Advanced — Monitor, Evaluate, Select

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — — Understand the in-place information security procedures and safeguards and the assignment of responsibilities to ensure that operations personnel are complying with them.

2. Intermediate — Provide leadership and direction to operations personnel by ensuring that information security awareness, basics and literacy, and training are provided to operations personnel commensurate with their responsibilities.

3. Advanced — Monitor and evaluate the effectiveness of information security procedures and safeguards to ensure they provide the intended level of protection. Take action as necessary should the level of protection fall below the established minimum.

Applicable Roles (minimum) —

Data Center Manager	Network Administrator	System Administrator
Senior Agency Information Security Officer/Manager and Staff		
Program and Functional Managers	Information System Security Officer	
Security Administrator	Information Owner	System Owner

INFORMATION SECURITY TRAINING TOPICS

4. System Interconnection
5. Information Sharing
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.4B)

Training Area: **Operations/Maintenance**
Responsibility: **Acquire**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The operations/maintenance phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

Behavioral Outcome — Individuals with acquisition responsibilities are able to understand the information security concerns associated with system operations and to identify and use the appropriate contract vehicle to meet current needs in a timely manner.

Knowledge Levels —

1. Beginning/Intermediate — Know, Review, Decide
3. Advanced — Determine, Interpret, Authorize

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate — Monitor contract performance and review deliverables for conformance with contract requirements related to information security and privacy.

3. Advanced — Take action as needed to ensure that accepted products/services meet contract requirements.

Applicable Roles (minimum) —

Contracting Officer	System Owner	Information Owner
Contracting Officer's Technical Representative (COTR)		
Senior Agency Information Security Officer/Manager and Staff		
Program and Functional Managers	Information System Security Officer	

INFORMATION SECURITY TRAINING TOPICS

8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64
NIST SP 800-36
NIST SP 800-35
NIST SP 800-23

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.4C)

Training Area: **Operations/Maintenance**
Responsibility: **Design & Develop**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The operations/maintenance phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

Behavioral Outcome — Individuals responsible for system development are able to make procedural and operational changes necessary to maintain the acceptable level of risk.

Knowledge Levels —

1. Beginning/Intermediate — Develop, Know, Understand
3. Advanced — Select, Analyze, Decide

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate — Design/develop new or modified information security procedures or safeguards to accommodate changes in operations.

3. Advanced — Modify/select information security procedures/safeguards that enhance the existing level of security and integrity.

Applicable Roles (minimum) —

Senior Agency Information Security Officer/Manager and Staff		
Network Administrator	System Administrator	Security Administrator
Programmer/Systems Analyst	Information System Security Officer	
System Designer/Developer	Systems Operations Personnel	
Authorizing Official		

INFORMATION SECURITY TRAINING TOPICS

3. System Environment
4. System Interconnection
5. Information Sharing
7. Risk Management
9. Acquisition/Development/Installation/Implementation Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64
NIST SP 800-53

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.4D)

Training Area: **Operations/Maintenance**
Responsibility: **Implement & Operate**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The operations/maintenance phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

Behavioral Outcome — Individuals responsible for system implementation or operation are able to maintain appropriate safeguards continuously within acceptable levels of risk.

Knowledge Levels —

1. Beginning — Know, Participate, Monitor
2. Intermediate — Evaluate, Identify, Execute
3. Advanced — Analyze, Interpret, Recommend

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in maintaining safeguards in accordance with standard operating procedures. Monitor system activity to identify potential information security events.

2. Intermediate — Evaluate potential information security events, identify actual security incidents, and take appropriate corrective and recovery actions.

3. Advanced — Analyze information security incidents or patterns of incidents to determine if remedial actions are needed to correct vulnerabilities and maintain the acceptable level of risk.

Applicable Roles (minimum) —

Database Administrator	Data Center Manager	Network Administrator
Senior Agency Information Security Officer/Manager and Staff		
System Administrator	Security Administrator	Technical Support Personnel
System Operations Personnel	Telecommunications Specialist	
Information System Security Officer	Incident Response Coordinator	
Risk / Vulnerability Analyst		

INFORMATION SECURITY TRAINING TOPICS

7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.4E)

Training Area: **Operations/Maintenance**
Responsibility: **Review & Evaluate**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The operations/maintenance phase includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

Behavioral Outcome — Individuals responsible for review and evaluation are able to examine the operational system to determine the adequacy and effectiveness of safeguards and to ensure that a consistent and appropriate level of security (i.e., one with an acceptable level of risk) is maintained.

Knowledge Levels —

1. Beginning — Understand, Participate, Identify
2. Intermediate — Analyze, Determine, Apply
3. Advanced — Decide, Recommend, Interpret

Terminal and Enabling Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Participate in the evaluation of an operational system to determine the adequacy and effectiveness of security safeguards and environment, leading to continued approval to operate (recertification and re-accreditation).
   - Understand – that any modifications to hardware and/or software may constitute a re-evaluation of the operational system to ensure appropriate level of security is maintained.
   - Participate – in the evaluation of the operational system to determine adequacy and effectiveness of security controls.
   - Identify – inadequacies that may exist (or may appear from modifications to hardware and/or software) in the information system.

2. Intermediate — Determine the adequacy of security environments and the capability of security strategies, architectures, and safeguards to maintain the integrity of those security environments. Prepare recommendations for system approval decisions.

- Analyze – the adequacy of security environments and the capability of security strategies, architectures, and safeguards to maintain the integrity of those security environments.
- Determine - the adequacy of security environments and the capability of security strategies, architectures, and safeguards to maintain the integrity of those security environments; prepare recommendations for system approval decisions.
- Apply – security strategies, architectures, and safeguards determined to maintain the integrity of the information system.

3. Advanced — Recommend IT system recertification/re-accreditation and/or corrective actions required to achieve/maintain certification/accreditation.

- Decide - if the assigned impact values with respect to the potential loss of confidentiality, integrity, and availability are consistent with the Agency's actual mission requirements.
- Recommend - IT system recertification/re-accreditation and/or corrective actions required to achieve/maintain certification/accreditation.
- Interpret – all documentation (covered in operations cell for this phase also).

Applicable Roles (minimum) —

Auditor, External	Auditor, Internal	First Responders
Senior Agency Information Security Officer/Manager and Staff		
Information System Security Officer	Office of the General Counsel Staff	
Agency Head / Other Executives	Risk / Vulnerability Analyst	
Security Engineer	Risk Executive	Assessor

INFORMATION SECURITY TRAINING TOPICS

7. Risk Management
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64

System Life Cycle Security (3.5A)

Training Area: **Disposal**
Responsibility: **Manage**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The disposal phase comprises the series of steps taken to retire a system when it is no longer needed and to securely and properly archive or dispose of its assets.

Behavioral Outcome — Individuals with management responsibilities are able to understand the special information security considerations and measures required during the shutdown of a system, and effectively plan and direct these activities.

Knowledge Levels —

1. Beginning — Understand, Apply, Monitor
2. Intermediate/Advanced — Validate, Decide, Direct, Approve

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Understand and ensure compliance with the information security considerations and procedures required for termination of the system.

2. Intermediate/Advanced — Ensure that appropriate and adequate plans and procedures are established, validate the termination plan, and accept the residual level of risk.

Applicable Roles (minimum) —

Database Administrator	Data Center Manager	Information Owner
Senior Agency Information Security Officer/Manager and Staff		
Program and Functional Managers	System Owner	
Information System Security Officer		

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
5. Information Sharing
6. Security Objectives
7. Risk Management

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.5D)

Training Area: **Disposal**
Responsibility: **Implement & Operate**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The disposal phase comprises the series of steps taken to retire a system when it is no longer needed and to securely and properly archive or dispose of its assets.

Behavioral Outcome — Individuals responsible for IT system operation are able to develop and implement the system termination plan, including security requirements for archiving/disposing of resources.

Knowledge Levels —

1. Beginning — Understand, Comply, Report
2. Intermediate — Apply, Decide, Conduct
3. Advanced — Analyze, Determine, Develop

Terminal Learning Objectives —
At the conclusion of this module, individuals will be able to:
1. Beginning — Comply with disposal procedures and report any potential information security incidents or actual breaches to proper authorities.
2. Intermediate — Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with the system disposal plan.
3. Advanced — Develop the system disposal plan to ensure that information security breaches are avoided during shutdown and long-term protection of archived resources is achieved.

Applicable Roles (minimum) —

Contracting Officer's Technical Representative		
Program and Functional Managers	Programmer/Systems Analyst	
Data Center Manager	Database Administrator	System Administrator
Records Management Official	Freedom of Information Act Official	
Senior Agency Information Security Officer/Manager and Staff		
Systems Operations Personnel	Technical Support Personnel	
Network Administrator	Security Administrator	Privacy Act Official
Information System Security Officer		

INFORMATION SECURITY TRAINING TOPICS

5. Information Sharing
6. Security Objectives
7. Risk Management

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64

INFORMATION SECURITY TRAINING
Curriculum Module
System Life Cycle Security (3.5E)

Training Area: **Disposal**
Responsibility: **Review & Evaluate**

Definition — The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model includes five phases: Initiation, Development/Acquisition, Implementation/Assessment, Operations/Maintenance, and Disposal. Life cycle security is the ensemble of processes and procedures which ensure data confidentiality, as needed, as well as data and system integrity, and availability.

The disposal phase comprises the series of steps taken to retire a system when it is no longer needed and to securely and properly archive or dispose of its assets.

Behavioral Outcome — Individuals responsible for review and evaluation are able to verify the appropriateness of the disposal plan and processes used to dispose of the IT system securely

Knowledge Levels —

1. Beginning/Intermediate/Advanced — Evaluate, Determine, Verify

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning/Intermediate/Advanced — Evaluate the disposal plan and procedures to ensure that information security and archival concerns have been appropriately addressed

Applicable Roles (minimum) —

Auditor, External	Auditor, Internal		First Responders
Information Resources Manager		Office of the General Counsel Staff	
Senior Agency Information Security Officer/Manager and Staff			
Information System Security Officer	Agency Head / Other Executives		Assessor
Risk Executive			

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
5. Information Sharing
6. Security Objectives
7. Risk Management

RESOURCE DOCUMENTS

NIST SP 800-18
NIST SP 800-64

Appendix C: Evaluating Training Effectiveness

Evaluate: "To determine or fix the value of; to examine carefully"

Value of Evaluation in a Training Program

Evaluating training effectiveness is a vital step to ensure that the training delivered is meaningful. Training is "meaningful" *only* when it meets the needs of both the student (employee) and the organization. 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, web-based training) is inappropriate, either in relation to the simplicity/complexity of the content or to the type of audience—or if there is an inadequate mix of vehicles in an agency's overall training program—the training will not meet needs. 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.

All meaningless training is expensive, even where the direct cost outlay, or cost-per-student, maybe low.   Because agencies cannot afford to waste limited resources on ineffective training, evaluation of training effectiveness should become an integral component of an agency's information security training program. A robust training evaluation effort may be the second most effective vehicle for garnering management support for information security—the first being the occurrence of a serious security incident.

In broader context, attention to information security training evaluation is in line with a changing focus in the overall field of information systems regarding how results of systems efforts are measured. The focus is beginning to change from being solely a machine view, i.e., measuring the functionality of the technology (e.g., speed, gigabytes), to encompass a people view, i.e., the functionality of the people who use the technology. Thus, in organizations where it is recognized that system utility is affected—or even determined—by users, it becomes apparent that to achieve its full utility, a percentage of the system budget must be devoted to people needs such as training.[4]

Purposes of Training Effectiveness Evaluation

Meaningfulness, or 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 effectiveness;

- A pattern of student 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 information security 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:

- First, evaluation should yield information to assist the employees themselves in assessing their subsequent on-the-job performance.

- Second, evaluation should yield information to assist the employees' supervisors in assessing individual students' subsequent on-the-job performance.

- Third, it should produce trend data to assist trainers in improving both learning and teaching.

- Finally, it should produce return-on-investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of information security awareness, awareness training (basics and literacy), role-based training, and education options for optimal results among the workforce as a whole.

Development of an Evaluation Plan

It is difficult to get "good" information for each of evaluation's four purposes (above). It is impossible to do so without planning for evaluation. To evaluate student learning, it is first necessary to have written learning objectives, stated in an observable, measurable way as behavioral outcomes: in short, "behavioral objectives." To evaluate teaching, it is necessary to plan for the collection of trend data, evaluation, and extrapolation. To evaluate return on investment, mission-related goals must be explicitly identified to which the learning objectives are related. *Thus, to obtain "good" information in each of these areas, the process of course development should include the development of an evaluation plan.* 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, Activity to be Performed, and Level of Success. 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. A "snowstorm" metaphor is illustrative. For meteorologists to forecast the arrival of a snowstorm, certain conditions must exist: e.g., relative humidity at a certain level, air temperature, conducive atmospheric conditions. Similarly, 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 computer-based training (CBT), not just "platform" training, must be specific and comprehensive. Keep in mind that if just one of the conditions for a snowstorm is missing, the storm either will not arrive or its force will be diminished. So, too, with learning.

- 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—whether 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 changing an 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 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 student response. 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.

- Level 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 information security 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—a subjective goal. 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 data to be collected are to be used to support the cost and effort of the data collection. This can be related to levels of evaluation, presented below.

Levels of Evaluation

Four levels of evaluation, in order of complexity, are:

- Level 1: End-of-Course Evaluations (Student Satisfaction)

- Level 2: Behavior Objective Testing (Learning Effectiveness, which is also a measure of Teaching Effectiveness)

- Level 3: Job Transfer Skills (Performance Effectiveness)

- Level 4: Organizational Benefit (Training Program Effectiveness)

Altogether, the four levels match the four purposes of training evaluation (described earlier in this appendix) in a staged manner. These levels are as follows.

- Level 1: End-of-Course Evaluations (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. For example, technical training provided to an audience of systems analysts and programmers will have a different level of effect than that provided to an audience of accountants. Basic demographic data may be collected at either course commencement or conclusion, but information regarding the learners' satisfaction with the course and course material should be collected at the end of the course.

- Level 2: Behavior Objective Testing (Learning and Teaching Effectiveness)

This level of evaluation measures how much information or skill was transmitted from the training activity to the learner. The evaluation should be in various formats relative to the level of training. In an awareness training course, for example, participants could be given a pre-test and a post-test of multiple choice items or fill-in-the-blank statements. 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. At the education level, essay questions exploring concepts would be appropriate. The evaluation format must relate back to the behavioral objectives of the learning activity which, in turn, drive the content being presented. The Level 2 evaluation also provides instant feedback, but it is more objective than a Level 1 evaluation: 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. As previously noted, Level 2 evaluation can be built into each block of instruction and does not need to wait until the end of a course.

A Level 2 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. 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 that the course 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, an approach is to use pre/post testing in which testing is performed at the outset, and the results are 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.

- Level 3: Job Transfer Skills (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 grade 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.

- Level 4: Organizational Benefit (Training Program Effectiveness)

Level 4 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 by a subject-matter expert of outputs produced by a student both before and after training. 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. Level 4 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 information security specialist in this organization, or to devote the same resources to security basics and literacy 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?" Determination of the purpose and objectives of a Level 4 evaluation, as well as the number of variables and the method of measurement of skill level, should only be done following completion of Level 3 evaluation(s), utilizing the findings thereof.

Implementation of Evaluation Planning

The information in Exhibit 8-1 should help in starting a comprehensive evaluation effort of an organization's information security training program. Each cell suggests the overall skill objective which should be attained by the cell evaluator (e.g., instructor, or the student's supervisor, as appropriate) and/or the overall program evaluator with respect to the various types of learning programs. Each cell also produces a variety of specific information and requires different tools.

Because of the vast amount of data collected, evaluation tools usually consist of a series of questions which require response on a Likert-type scale.   This scale, from one to five (one being very good; five being not good, or vice versa), allows the evaluator to prioritize the usefulness of the overall training program and the specific courses or learning events or components within it. Each tool is program- and site-specific.

A practical method to use is to choose a starting point in Exhibit F-1, beginning with a type of training the organization currently offers; then find an evaluation tool appropriate to a cell at that level and borrow or adapt the concepts presented from already-developed tools. Samples of some of these evaluation tools appear as Exhibits C-2 and C-3. Agency training staff may be able to help locate other tools.

Evaluation Objectives				
Levels of Evaluation Student	Level 1: Satisfaction	Level 2: Learning Effectiveness	Level 3: Performance Effectiveness	Level 4: Training Program Effectiveness
Type of Training Basics/Literacy	How well did the student think he/she grasped the security concepts? For CBT, how many attempts did it take for the student to pass the test?	How did the majority of students perform on the test, e.g., do aggregated post-test answers show sufficient improvement over pre-test answers?	How well is the student using the core skill set in his or her daily activities routine?	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?
Training	How well did the training program fit the student's expectations?	Did the training program demonstrably and sufficiently increase the scope and/or depth of the student's skill set?	How well is the student applying the new security skills to functional job requirements?	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?
Education	Did the course of study advance the student's career development or professional qualifications in information security?	Could the student apply the increased knowledge to a real world situation adequately?	How well is the student's acquired information security 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 C-1 Evaluation Objectives

Sample Questionnaire — Level 1 Evaluation Training Assessment by Student

1. Indicate your highest level of education:

    High School graduate or less   Bachelor's Degree
    Some college/technical school   Master's Degree
    Associate degree or technical certification   Doctorate

2. 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

3. 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

4. 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

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

    Too elementary   Somewhat difficult   About right
    Somewhat elementary   Too difficult

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

    Too slow   Somewhat fast   About right
    Somewhat slow   Too fast

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

    Light
    About right
    Heavy

8. Considering my previous experience with this subject matter, the course content was:

    Out of date
    Somewhat current
    Current

9. 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

Student Perception of Instructor

Extent to which the instructor successfully:	Excellent	Good	Fair	Poor	N/A
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
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)

2. 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

3. 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

4. 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 information 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 information security-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

2. 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.

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

    I had read the catalog description or brochure and knew the expected behavioral outcome.
    I had read the catalog description or brochure but did not know the expected behavioral outcome.
    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 behavioral outcome.
    I only knew the course existed.
    I knew nothing about the course until I received this form.

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

Highly satisfied
Satisfied
Dissatisfied
Highly dissatisfied
Unsure

Exhibit C-3 Sample Questionnaire — Level 3 Evaluation Training Assessment by Supervisor

Summary

Evaluation is undertaken to measure the effectiveness of an agency's or organization's information security training program, i.e., the extent to which the overall program and its respective components are either meaningful or a waste of the organization's limited training resources. The employee (student) must be asked their view of each learning event (Level 1 and Level 2), the supervisor their view of the event (Level 3), and the organization its view of the event (Level 4) in relation to return on investment. In this process, both quantitative and qualitative data will be collected. At Levels 3 and 4, data collection will be longitudinal. As important as it is for the evaluator to collect the raw data, analysis and application of the collected data is where the SAISO and senior officials get the organization's money's worth out of its information security training program. Evaluation planning in advance of the event(s) to be evaluated is essential.