FISSEA
2005

Security Is Everyone’s Business: Role-Based Training for The System Development Life Cycle

Prepared for: **FISSEA 2005**

Prepared by: **Mrs. Margaret K. Spanninger**

Booz Allen Hamilton
3190 Fairview Park Drive
Falls Church, Virginia 22042

e-mail: spanninger_margaret@bah.com
v-mail: (703) 289-5471
fax: (703) 289-5829

Abstract: This paper is based on the premise that the integration of security into organizational business processes, especially the system development life cycle (SDLC), is a fundamental requirement for Federal Information Security Management Act (FISMA) compliance and attaining security performance goals. Now, more than ever, security role-based training is key for achieving security integration into enterprise business processes and the cultural change that is required to sustain long-term organizational benefits and improvement in enterprise security programs.

Organizations must identify the stakeholders in each life cycle phase and educate them about their roles. This education must help personnel distinguish between performance and compliance issues, and the roles responsible and accountable for “doing” security versus “ensuring” security. Role-based training will address these stakeholders and their roles and teach them what is required to pass the “security baton” from one phase to the next.

By integrating security into the SDLC and providing role-based training to personnel with significant security responsibilities, organizations can be better prepared to meet the challenges of FISMA compliance. It is clear that IT systems cannot be adequately protected unless all personnel understand their roles and responsibilities for safeguarding the information and information resources. Training can promote cultural change and shift the workforce from being observers who show interest in security to becoming participants who demonstrate commitment to security.

This paper focuses on developmental activities of the SDLC, security activities that must be integrated into the SDLC, and the players or stakeholders in each SDLC phase. It is only through the understanding of these security roles and their relationships among each other that total security integration can occur.

Biography

Margaret (Marge) Spanninger is an Associate at Booz Allen Hamilton Inc. where she leads the Security Workforce Development Services group of Booz Allen's Global Resilience Team. She was graduated from West Virginia Wesleyan College with a B.S. in Accounting and from The George Washington University with an M.B.A in Information Systems Technology. Mrs. Spanninger has over 25 years of experience in technical and security training design, development, and delivery. She has conducted security training for government clients that include Department of Veterans Affairs, Department of Energy, Department of Education, General Services Administration, and several agencies of the Intelligence Community.

Mrs. Spanninger is the author of the following papers—

Developing Security Competencies Through Information Assurance Undergraduate and Graduate Programs, presented at the National Colloquium for Information System Security Educators (NCISSE) Conference, September 2001.

Security Awareness and Training: The Neglected Countermeasures, presented at the Federal Information System Security Educators Association (FISSEA), March 2003.

INTRODUCTION

Integration of security into the SDLC is one of the key elements required for resolving many of the long-standing weaknesses in information technology (IT) security and achieving sustainable performance improvements in IT security programs. FISMA states under §3544. Federal agency responsibilities (b) AGENCY PROGRAM—

> "Each agency shall develop, document, and implement an agency-wide information security program that includes…(2) policies and procedures that…(C) ensure that information security is addressed throughout the life cycle of each agency information system."

Including security early and throughout the SDLC is a primary means for meeting security assurance requirements and ensuring a less expensive and more effective implementation than adding security to an operational system. Process re-engineering is required to effect security integration throughout the SDLC. As a result, personnel must be continually trained in the new processes and corresponding security tasks.

BUSINESS DRIVERS

Personnel at all levels must understand that "security is not an option;" it is an integral element of all IT systems. Performing security activities within each phase of the SDLC will not only improve IT security, it will improve the bottom line. There are several business factors that underscore the importance of integrating security activities within the SDLC. First, security is less expensive to implement if it is planned from the beginning because it reduces the need for expensive reengineering and reprogramming in later phases. Reducing costs is important to any organization and the savings that are realized can be applied to other needs. Second, building security controls into the system, rather than adding them after the system is already built, improves system performance. The performance gains that result from integrating security early will directly improve productivity and user satisfaction. Third, introducing security countermeasures early removes the stigma that security is a barrier to success. Addressing security early helps promote it as an "enabler" as opposed to a "necessary evil." Finally, security integration facilitates and ensures the success of certification and accreditation (C&A) as security deficiencies are reduced or eliminated. Time and effort to remediate vulnerabilities is decreased and additional savings are realized through stringent configuration management. This success will be realized on new systems transitioning from implementation/integration status to becoming fully operational and will continue throughout the system's life. These factors enable secure business processes and provide assurance that business and mission objectives can be met with acceptable risk.

Organizations have proven repeatedly over the years that if security is not identified as a requirement, it will not be addressed. As we learn from our mistakes, we will realize that it is critical to plan for countermeasures in the earliest phases—before implementation—to ensure:

1) adequate and appropriate resources are allocated for security throughout the system's life;

2) a structured and consistent approach for developing and maintaining security for IT systems;

3) the most cost-effective security controls are chosen and implemented; and

4) increased homogeneity among information systems and security controls within an organization to reduce operational costs.

To understand what must be done from a security perspective, one must first understand what happens in each phase of the SDLC.

SYSTEM DEVELOPMENT LIFE CYCLE

There are several models that support SDLC concepts: the traditional linear model, the prototyping model, the spiral model, the component assembly model, and the concurrent development model. Although the models have evolved to match the dynamics of the technology and the complexity of the implementation, the underlying foundation remains universal and can be applied within each model. This foundation is composed of five phases: initiation, development/acquisition, implementation/integration, operations and maintenance, and disposition.

The initiation phase is where the idea for a new system, enhancements to a system, or expansion of a system originates—someone thinks there is a need. Before the need is actually addressed, basic questions must be answered. How does the change support the business or mission? Is there capacity available on existing resources? If not, do we have the budget, time, and personnel to explore alternatives and move forward? If the decision is made to move forward, requirements must be collected and documented. These requirements feed the acquisition/development phase where a build or buy decision is made and paperwork is generated to support the acquisition process for products and services. Next, the products and services are implemented and/or integrated with the existing system and environment. Once the new system is tested and deemed to be ready operationally, it is transitioned from the integration environment to the operational environment. It is now in maintenance mode and adjustments are made when necessary. Finally, the system is removed from service when it can no longer meet business needs or demands.

Regardless of the SDLC model that is used, security must be integrated within each phase and responsibility for security must pass seamlessly between the phases. The National Institute of Standards and Technology (NIST) provides guidelines to the Federal sector for implementing IT security. Their Special Publication (SP) 800-64, *Security Considerations in the Information System Development Life Cycle*, describes baseline security activities that should be performed in each phase of the SDLC. Exhibit 1 identifies these baseline activities.

Exhibit 1. Security Activities Mapped to SDLC Phases

SDLC PHASE	SECURITY ACTIVITIES
Initiation	• Determine needs • Perform the security categorization • Perform a risk assessment
Development/ Acquisition	• Analyze, define, and document security functional requirements • Analyze, define, and document security assurance requirements • Identify cost considerations • Develop security control(s) • Create the developmental Security Test and Evaluation Plan • Perform a risk assessment • Create acquisition specifications and documentation
Implementation/ Integration	• Perform inspection and acceptance procedures for security controls • Perform security integration processes and procedures • Perform certification processes and procedures • Perform accreditation processes and procedures
Operations and Maintenance	• Define and implement configuration management and controls • Perform continuous monitoring (recertification and re-accreditation)
Disposition	• Preserve information • Sanitize media • Dispose of hardware and software

PERSONNEL WITH SIGNIFICANT SECURITY RESPONSIBILITY

Security cannot be integrated into the SDLC successfully until people with significant security responsibilities are identified and trained to perform their security duties. Authority for training personnel in these duties resides with the Chief Information Officer (CIO) as specified under FISMA, which states in §3544. Federal agency responsibilities (a) IN GENERAL.—The head of each agency shall—

> "(3) delegate to the agency Chief Information Officer…the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—…(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;
>
> (4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines;…"

The Office of Personnel Management (OPM) revised 5 Congressional Federal Register (CFR) part 930, subpart C, in June 2004 to clarify security awareness and training requirements for the Federal sector. This regulation also requires each Executive Agency to "identify employees with significant information security responsibilities and provide role-specific training in accordance with NIST standards and guidance." 5CFR part 930.301 Computer security training program states—

> "(1) All users of information technology (IT) shall be exposed to security awareness materials at least annually. Users of IT include employees, contractors, students, guest researchers, visitors and others who may need access to IT systems and applications.
>
> (2) Executives shall receive training in computer security basics and policy level training in security planning and management.
>
> (3) Program and functional managers shall receive training in computer security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
>
> (4) Chief Information Officers (CIO), IT security program managers, auditors and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) shall receive training in computer security basics; and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
>
> (5) IT function management and operations personnel shall receive training in computer security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning."

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, identifies 26 job positions that have significant security responsibilities. I have grouped these positions into seven (7) functional roles. Unlike NIST, I make a distinction between executives and managers. Exhibit 2 identifies the job positions from NIST SP 800-16 aligned with the following functional roles: executive, manage, acquisition, system design/development, implementation/operations, compliance, and system user.

Exhibit 2. Positions Mapped to Functional Roles

FUNCTIONAL ROLES	POSITIONS
Executive	• Chief Information Officer • Senior Information Resource Management Official
Management	• System Owner (Business Manager) • Program Manager • Information Resource Manager • Records Management Official • Freedom of Information Act (FOIA) Official • Privacy Act Official
Acquisition	• Source Selection Board • Contracting Officer • Contracting Officer's Technical Representative (COTR)
System Design/Development	• System Designer/Developer • System/Program Analyst
Implementation/ Operations	• Data Center Manager • Network Administrator • System Administrator • Database Administrator • Technical Support (Helpdesk) • System Operator • Telecommunications Specialist
Compliance	• Designated Approving Authority (DAA) • Certification Reviewer • Information Security Officer/Information Security Manager • Auditor, Internal • Auditor, External
User	• Any position that uses information technology resources

To achieve a security solution that is not an option, but rather an integral part of the system, risk management and C&A activities must be performed throughout a system's life. It is critical that personnel in positions with significant security responsibilities actively participate in the SDLC. Their participation provides assurance that—

1) security requirements have been addressed;

2) countermeasures have been identified;

3) controls have been properly implemented and tested;

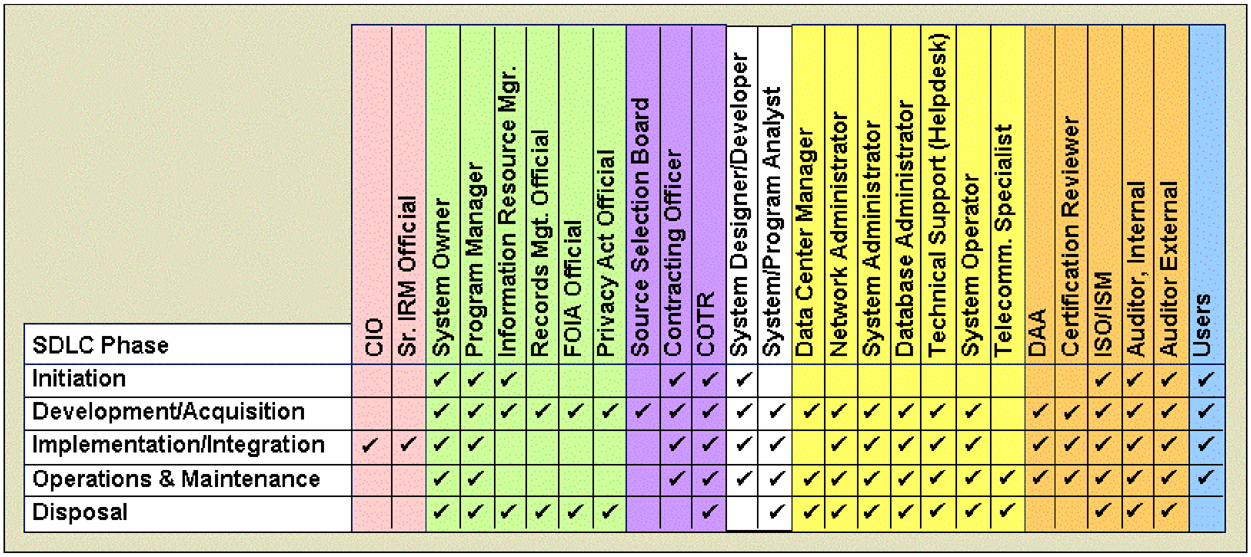
4) all changes to the operational system are reviewed to ensure the integrity of the system and security solution that have been certified and accredited; and

5) the data, hardware, software, and documentation are disposed of properly.

To accomplish this, organizations must attend to the "people" requirements that support security compliance throughout the system life cycle. Organizations must identify the stakeholders in each life cycle phase and educate them on their roles. This education must help personnel distinguish between performance and compliance issues, and the roles responsible and accountable for "doing" security versus "ensuring" security.

Role-based training must address the needs of these stakeholders and their roles and teach them what is required to pass the "security baton" from one SDLC phase to the next. Exhibit 3 identifies the NIST job positions mapped to the SDLC.

Exhibit 3. Positions Mapped to SDLC



SDLC Phase	CIO	Sr. IRM Official	System Owner	Program Manager	Information Resource Mgr.	Records Mgt. Official	FOIA Official	Privacy Act Official	Source Selection Board	Contracting Officer	COTR	System Designer/Developer	System/Program Analyst	Data Center Manager	Network Administrator	System Administrator	Database Administrator	Technical Support (Helpdesk)	System Operator	Telecomm. Specialist	DAA	Certification Reviewer	ISO/ISM	Auditor, Internal	Auditor External	Users
Initiation			✓	✓	✓					✓	✓	✓											✓	✓	✓	✓
Development/Acquisition			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Implementation/Integration	✓	✓	✓	✓						✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Operations & Maintenance			✓	✓						✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Disposal			✓	✓	✓	✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	

The "checks" shown in the matrix only apply to security responsibilities within the SDLC and do not extend beyond this scope. Many executives, senior officials, and business managers are involved with security from program management and planning perspectives, which extends beyond the SDLC.

ROLE-BASED TRAINING AND ASSURANCE

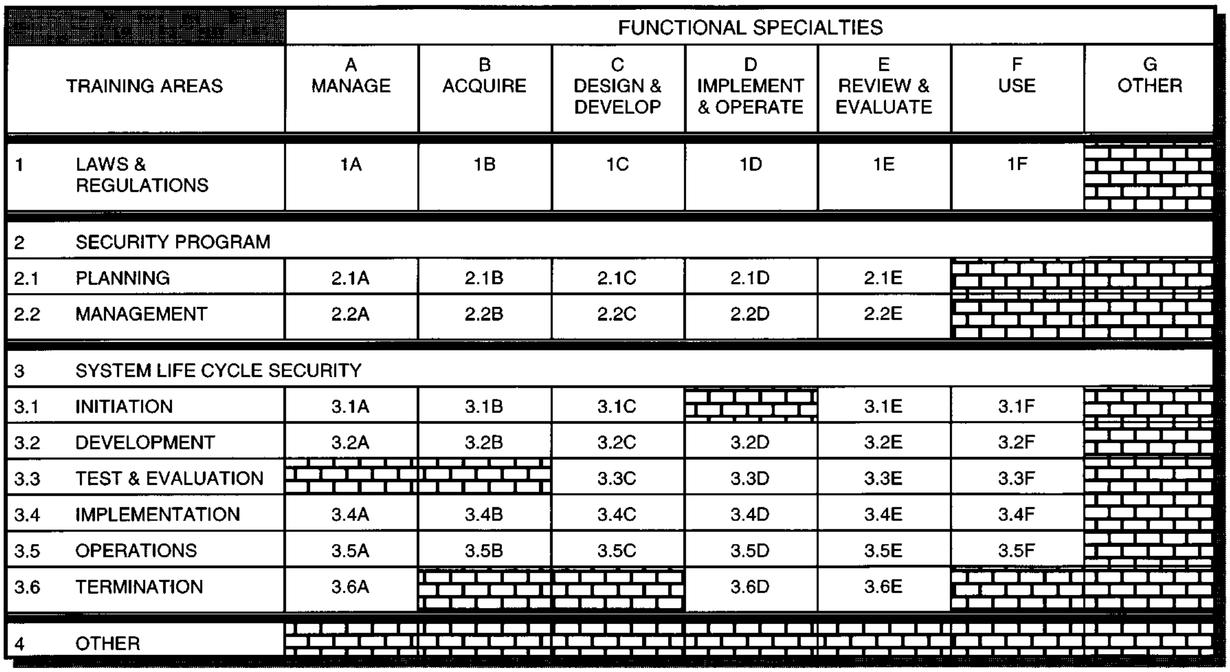
Role-based training plays a significant role in providing assurance. It is critical that all personnel in positions with significant security responsibility understand their security role in each phase of the life cycle and that they have the knowledge, skill and ability to perform the requisite security tasks of their position. Most personnel tend to focus on their security responsibilities for operational systems. This is a good step in the right direction because the majority of systems that are in place today spend the largest portion of their "life" in the operations and maintenance phase. It is important to recognize that the system that becomes operational today will not be the same as the system that is removed from service 10 – 15 years from now. As with everything else, the only constant is change. The system will undergo revisions, enhancements, and component replacement. New technologies will be integrated and obsolete technologies will be retired. It is for this reason that configuration management control and on-going C&A evaluation play such a pivotal role in maintaining the security of our systems. However, having the knowledge and skill to perform security duties in the operations phase is not enough. The workforce must be skilled in their security duties throughout the system's life as the security activities that must be performed in the other SDLC phases are repeated on a smaller scale within the operations and maintenance phase.

The primary goal of NIST SP 800-16 is to help agencies develop a comprehensive IT security training program which supports the missions of the organization and is administered as an integral element of sound IT management and planning. NIST SP 800-16 contains a wealth of information that can be extracted and put to good use if one is willing to invest some time to put all the pieces together. The guide identifies—

- three primary categories of security knowledge: laws and regulations, security programs with two sub-categories, and security in the SDLC with six subcategories;
- six functional roles: manage, acquire, design and develop, implement and operate, review and evaluate, and use, which are associated with each of the primary categories;
- twenty-six positions with significant security responsibilities;
- twelve topics that define a core body of knowledge for information security—
  - Laws and regulations
  - IT security programs
  - System environment
  - System interconnection (physical access)
  - Information sharing (logical access)
  - Sensitivity
  - Risk management
  - Life cycle controls
  - Management controls
  - Operational controls
  - Technical controls
  - Awareness, training and education

Exhibit 4, from NIST SP 800-16, pulls all the pieces together. The matrix illustrates the primary categories and subcategories as rows and the six functional roles as columns. This representation identifies 46 "cells." Each cell is linked to one or more of the core body of knowledge topics and to one or more position with significant security responsibilities.

Exhibit 4. IT Security Training Matrix

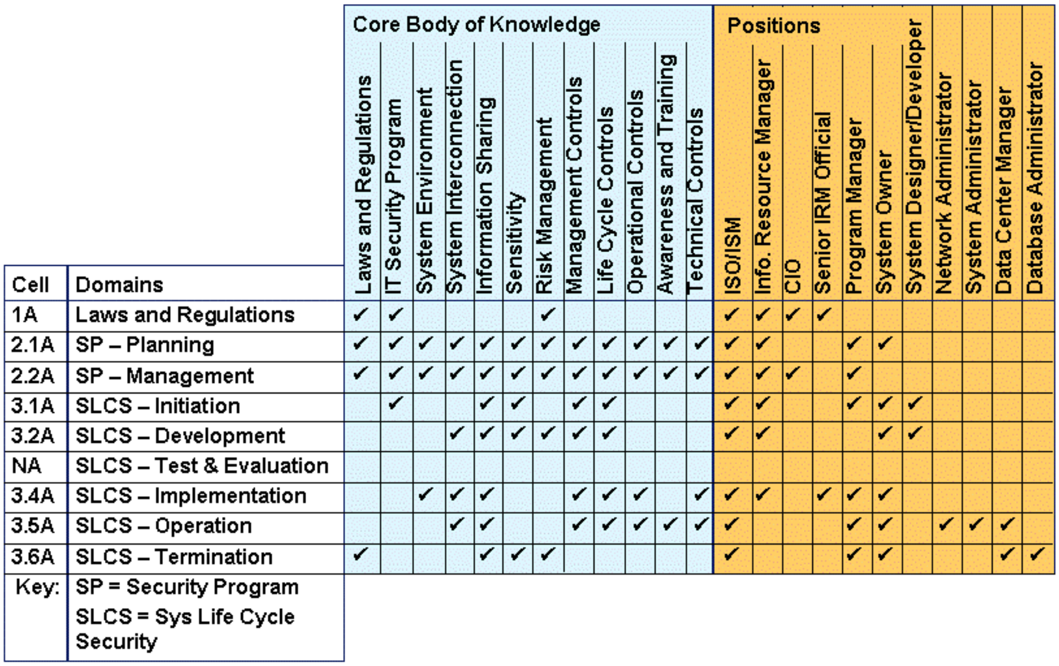


		FUNCTIONAL SPECIALTIES						
	TRAINING AREAS	A MANAGE	B ACQUIRE	C DESIGN & DEVELOP	D IMPLEMENT & OPERATE	E REVIEW & EVALUATE	F USE	G OTHER
1	LAWS & REGULATIONS	1A	1B	1C	1D	1E	1F	▨
2	SECURITY PROGRAM							
2.1	PLANNING	2.1A	2.1B	2.1C	2.1D	2.1E	▨	▨
2.2	MANAGEMENT	2.2A	2.2B	2.2C	2.2D	2.2E	▨	▨
3	SYSTEM LIFE CYCLE SECURITY							
3.1	INITIATION	3.1A	3.1B	3.1C	▨	3.1E	3.1F	▨
3.2	DEVELOPMENT	3.2A	3.2B	3.2C	3.2D	3.2E	3.2F	▨
3.3	TEST & EVALUATION	▨	▨	3.3C	3.3D	3.3E	3.3F	▨
3.4	IMPLEMENTATION	3.4A	3.4B	3.4C	3.4D	3.4E	3.4F	▨
3.5	OPERATIONS	3.5A	3.5B	3.5C	3.5D	3.5E	3.5F	▨
3.6	TERMINATION	3.6A	▨	▨	3.6D	3.6E	▨	▨
4	OTHER	▨	▨	▨	▨	▨	▨	▨

Although the NIST guide is organized by the primary categories (rows of the matrix), information presented here is organized by the functional roles (columns of the matrix). With this focus, one can easily discern the training needs for each functional role and the positions associated with each role.

The "manage role" is shown in Exhibit 5 to illustrate the functional orientation. It identifies the eight cells that support the manage role, the core body of knowledge associated with each domain (e.g., laws and regulations, security program, system life cycle security), and the 16 positions with "manage" responsibilities.

Exhibit 5. Manage Role



		Core Body of Knowledge												Positions										
Cell	Domains	Laws and Regulations	IT Security Program	System Environment	System Interconnection	Information Sharing	Sensitivity	Risk Management	Management Controls	Life Cycle Controls	Operational Controls	Awareness and Training	Technical Controls	ISO/ISM	Info. Resource Manager	CIO	Senior IRM Official	Program Manager	System Owner	System Designer/Developer	Network Administrator	System Administrator	Data Center Manager	Database Administrator
1A	Laws and Regulations	✓	✓					✓						✓	✓	✓	✓							
2.1A	SP – Planning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓					
2.2A	SP – Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓						
3.1A	SLCS – Initiation		✓			✓	✓		✓	✓				✓	✓			✓	✓	✓				
3.2A	SLCS – Development				✓	✓	✓	✓	✓	✓				✓	✓				✓	✓				
NA	SLCS – Test & Evaluation																							
3.4A	SLCS – Implementation			✓	✓	✓			✓	✓	✓		✓	✓	✓		✓	✓	✓					
3.5A	SLCS – Operation				✓	✓			✓	✓	✓	✓	✓	✓				✓	✓		✓	✓	✓	
3.6A	SLCS – Termination	✓				✓	✓	✓						✓				✓	✓				✓	✓
Key:	SP = Security Program SLCS = Sys Life Cycle Security																							

An addendum has been provided with this paper that illustrates the individual matrices for each functional role. Each matrix contains the cell identification from NIST SP 800-16 mapped to the 12 core body of knowledge topics and the appropriate positions with significant security responsibilities. These matrices are intended to answer the questions "What are the positions with significant security responsibilities?" and "What training is required for personnel who are in these positions?"

SUMMARY

By integrating security into the SDLC and providing role-based training to personnel with significant security responsibilities, organizations can be better prepared to meet the challenges of FISMA compliance. It is clear that IT systems cannot be adequately protected unless all personnel understand their roles and responsibilities for safeguarding the information and information resources. Training can promote cultural change and shift the workforce from being observers who show interest in security to becoming participants who demonstrate commitment to security. It is only through the understanding of these security roles and their relationships among each other and across the life cycle that total security integration can occur.

REFERENCES

Federal Information Security Management Act of 2002.

Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

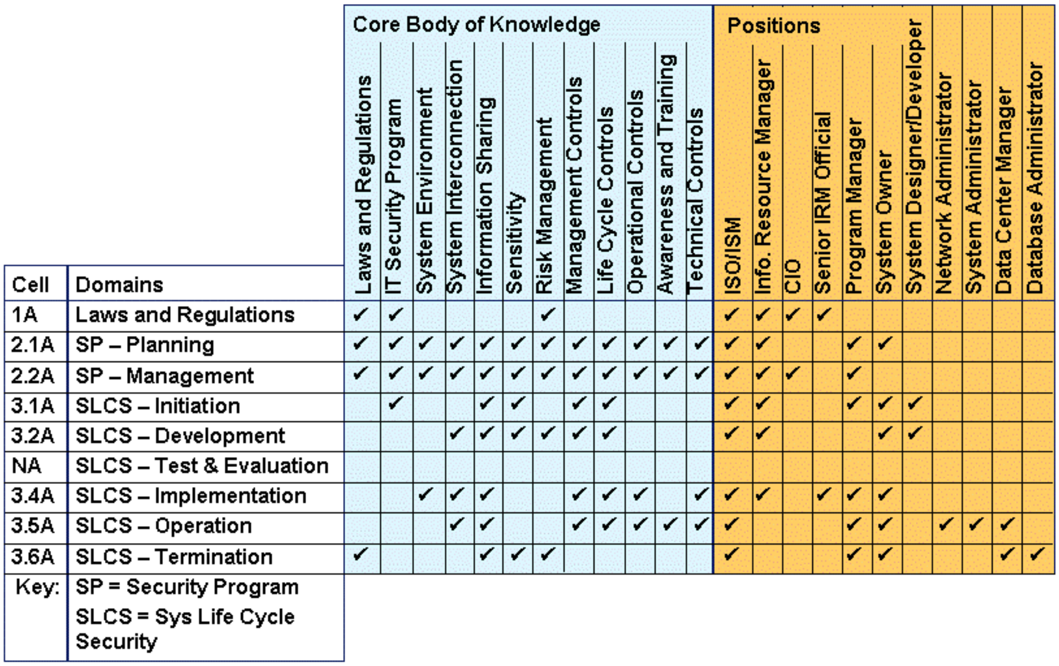
Office of Personnel Management, 5 Congressional Federal Register (CFR) part 930, subpart C, June 2004.

National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations for the Information System Development Life Cycle*, June 2004.

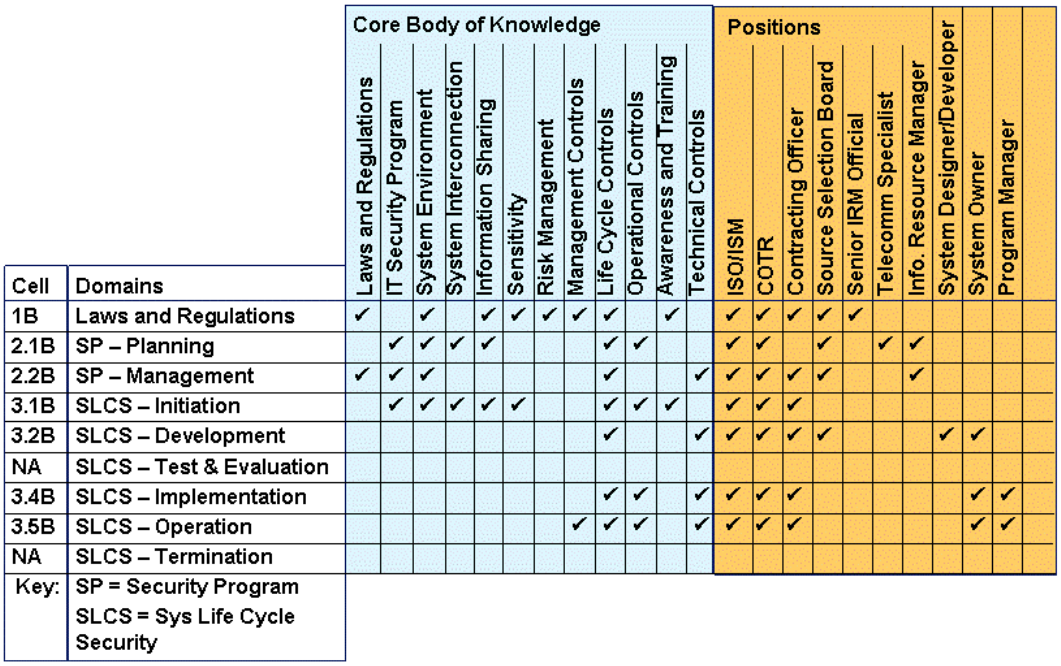
Addendum
Functional Training Matrices Mapped to Security Core Body of Knowledge and Positions with Significant Security Responsibilities

Manage Role



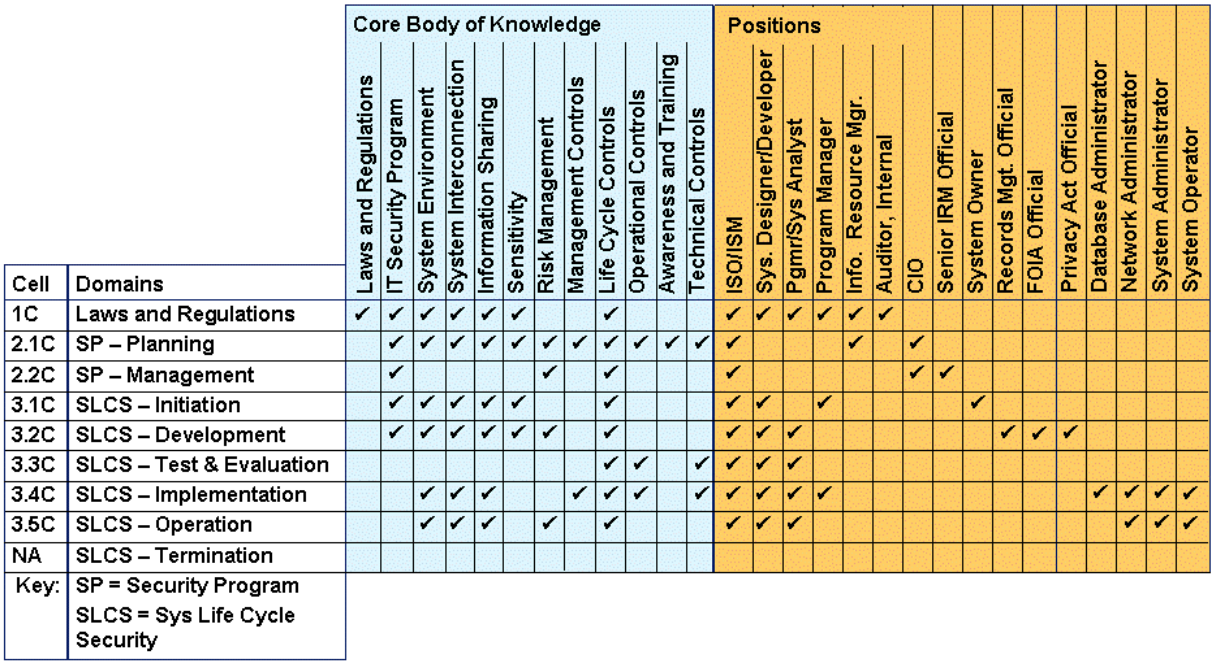
		Core Body of Knowledge												Positions										
Cell	Domains	Laws and Regulations	IT Security Program	System Environment	System Interconnection	Information Sharing	Sensitivity	Risk Management	Management Controls	Life Cycle Controls	Operational Controls	Awareness and Training	Technical Controls	ISO/ISM	Info. Resource Manager	CIO	Senior IRM Official	Program Manager	System Owner	System Designer/Developer	Network Administrator	System Administrator	Data Center Manager	Database Administrator
1A	Laws and Regulations	✓	✓					✓						✓	✓	✓	✓							
2.1A	SP – Planning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓					
2.2A	SP – Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓						
3.1A	SLCS – Initiation		✓			✓	✓		✓	✓				✓	✓			✓	✓	✓				
3.2A	SLCS – Development				✓	✓	✓	✓	✓	✓				✓	✓				✓	✓				
NA	SLCS – Test & Evaluation																							
3.4A	SLCS – Implementation			✓	✓	✓			✓	✓	✓		✓	✓	✓		✓	✓	✓					
3.5A	SLCS – Operation				✓	✓			✓	✓	✓	✓	✓	✓				✓	✓		✓	✓	✓	
3.6A	SLCS – Termination	✓				✓	✓	✓						✓				✓	✓				✓	✓
Key:	SP = Security Program SLCS = Sys Life Cycle Security																							

Acquire Role



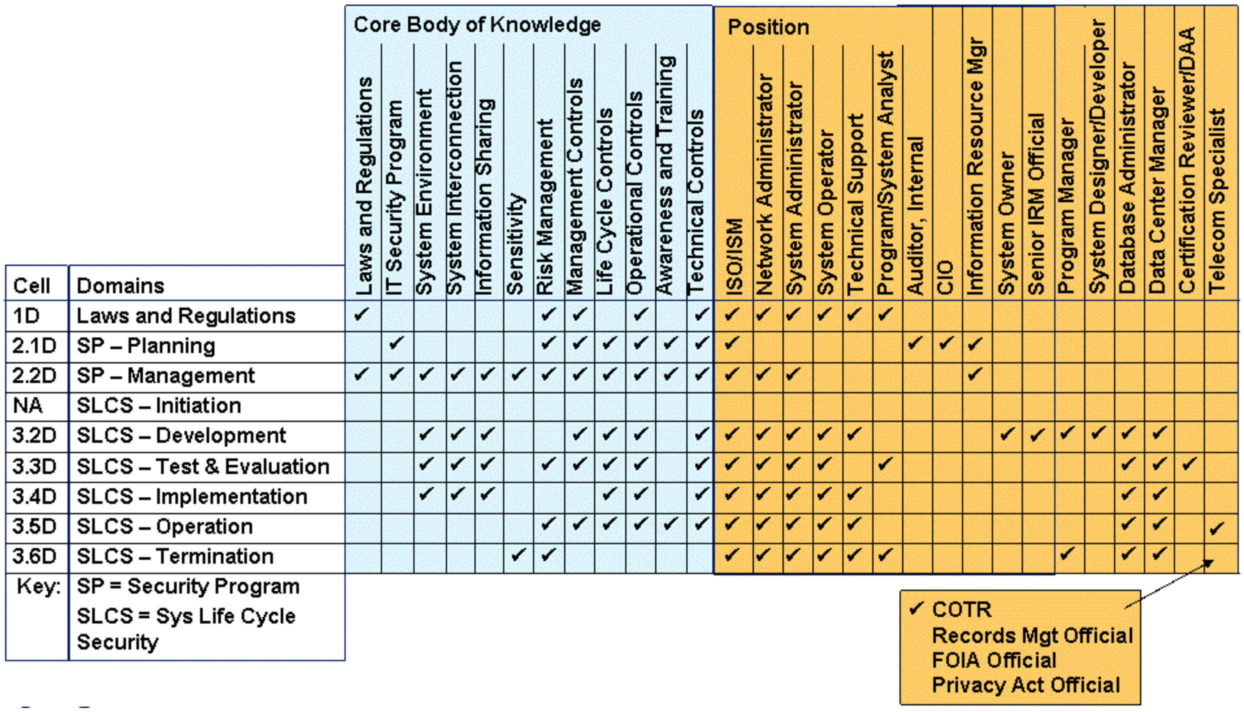
		Core Body of Knowledge												Positions										
Cell	Domains	Laws and Regulations	IT Security Program	System Environment	System Interconnection	Information Sharing	Sensitivity	Risk Management	Management Controls	Life Cycle Controls	Operational Controls	Awareness and Training	Technical Controls	ISO/ISM	COTR	Contracting Officer	Source Selection Board	Senior IRM Official	Telecomm Specialist	Info. Resource Manager	System Designer/Developer	System Owner	Program Manager	
1B	Laws and Regulations	✓		✓		✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓						
2.1B	SP – Planning		✓	✓	✓	✓				✓	✓			✓	✓		✓		✓	✓				
2.2B	SP – Management	✓	✓	✓						✓			✓	✓	✓	✓	✓			✓				
3.1B	SLCS – Initiation		✓	✓	✓	✓	✓			✓	✓	✓		✓	✓	✓								
3.2B	SLCS – Development									✓			✓	✓	✓	✓	✓				✓	✓		
NA	SLCS – Test & Evaluation																							
3.4B	SLCS – Implementation									✓	✓		✓	✓	✓	✓						✓	✓	
3.5B	SLCS – Operation								✓	✓	✓		✓	✓	✓	✓						✓	✓	
NA	SLCS – Termination																							
Key:	SP = Security Program SLCS = Sys Life Cycle Security																							

Design and Develop Role



		Core Body of Knowledge												Positions															
Cell	Domains	Laws and Regulations	IT Security Program	System Environment	System Interconnection	Information Sharing	Sensitivity	Risk Management	Management Controls	Life Cycle Controls	Operational Controls	Awareness and Training	Technical Controls	ISO/ISM	Sys. Designer/Developer	Pgmr/Sys Analyst	Program Manager	Info. Resource Mgr.	Auditor, Internal	CIO	Senior IRM Official	System Owner	Records Mgt. Official	FOIA Official	Privacy Act Official	Database Administrator	Network Administrator	System Administrator	System Operator
1C	Laws and Regulations	✓	✓	✓	✓	✓	✓			✓				✓	✓	✓	✓	✓	✓										
2.1C	SP – Planning		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓		✓									
2.2C	SP – Management		✓					✓		✓				✓						✓	✓								
3.1C	SLCS – Initiation		✓	✓	✓	✓	✓			✓				✓	✓		✓					✓							
3.2C	SLCS – Development		✓	✓	✓	✓	✓	✓		✓				✓	✓	✓							✓	✓	✓				
3.3C	SLCS – Test & Evaluation									✓	✓		✓	✓	✓	✓													
3.4C	SLCS – Implementation			✓	✓	✓			✓	✓	✓		✓	✓	✓	✓	✓									✓	✓	✓	✓
3.5C	SLCS – Operation			✓	✓	✓		✓		✓				✓	✓	✓											✓	✓	✓
NA	SLCS – Termination																												
Key:	SP = Security Program SLCS = Sys Life Cycle Security																												

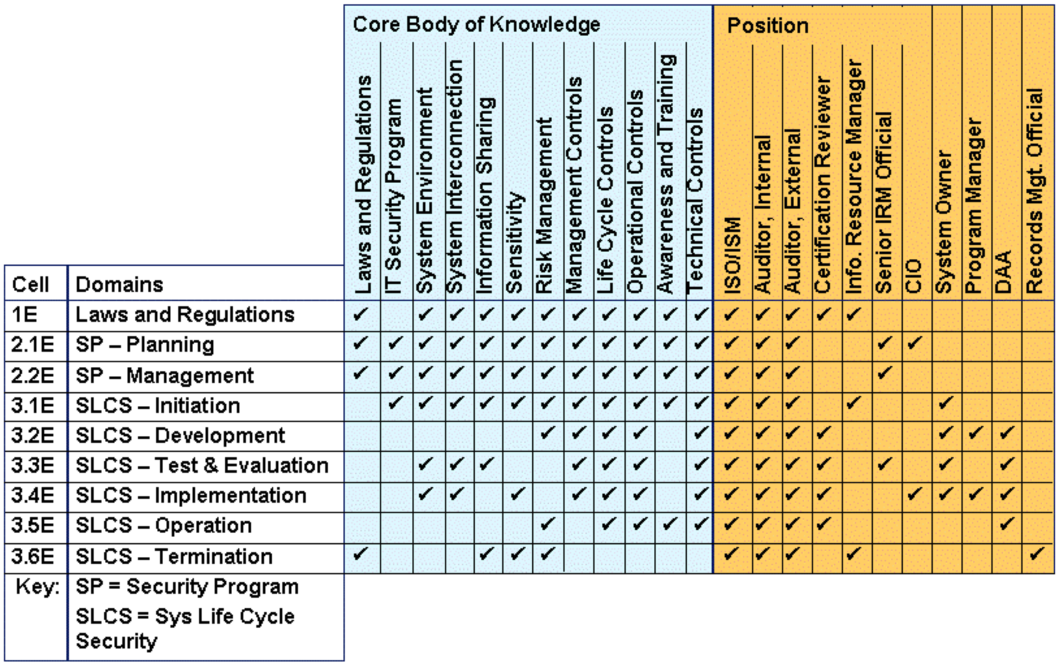
Implement and Operate Role



		Core Body of Knowledge												Position																
Cell	Domains	Laws and Regulations	IT Security Program	System Environment	System Interconnection	Information Sharing	Sensitivity	Risk Management	Management Controls	Life Cycle Controls	Operational Controls	Awareness and Training	Technical Controls	ISO/ISM	Network Administrator	System Administrator	System Operator	Technical Support	Program/System Analyst	Auditor, Internal	CIO	Information Resource Mgr	System Owner	Senior IRM Official	Program Manager	System Designer/Developer	Database Administrator	Data Center Manager	Certification Reviewer/DAA	Telecom Specialist
1D	Laws and Regulations	✓						✓	✓		✓		✓	✓	✓	✓	✓	✓	✓											
2.1D	SP – Planning		✓					✓	✓	✓	✓	✓	✓	✓						✓	✓	✓								
2.2D	SP – Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓						✓								
NA	SLCS – Initiation																													
3.2D	SLCS – Development			✓	✓	✓			✓	✓	✓		✓	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓		
3.3D	SLCS – Test & Evaluation			✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓		✓								✓	✓	✓	
3.4D	SLCS – Implementation			✓	✓	✓				✓	✓		✓	✓	✓	✓	✓	✓									✓	✓		
3.5D	SLCS – Operation							✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓									✓	✓		✓
3.6D	SLCS – Termination						✓	✓						✓	✓	✓	✓	✓	✓						✓		✓	✓		
Key:	SP = Security Program SLCS = Sys Life Cycle Security																													

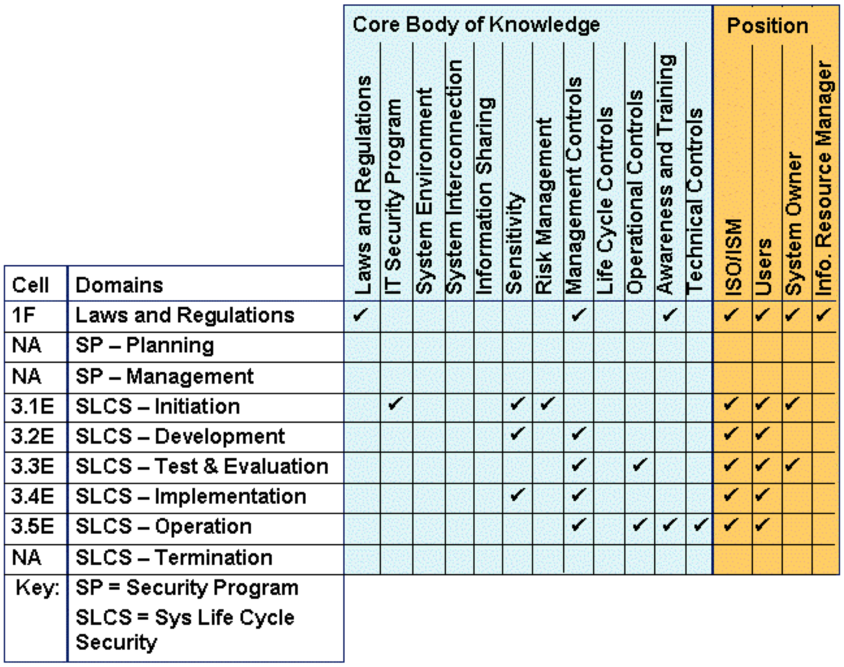
✓ COTR
Records Mgt Official
FOIA Official
Privacy Act Official

Review and Evaluate Role



		Core Body of Knowledge												Position										
Cell	Domains	Laws and Regulations	IT Security Program	System Environment	System Interconnection	Information Sharing	Sensitivity	Risk Management	Management Controls	Life Cycle Controls	Operational Controls	Awareness and Training	Technical Controls	ISO/ISM	Auditor, Internal	Auditor, External	Certification Reviewer	Info. Resource Manager	Senior IRM Official	CIO	System Owner	Program Manager	DAA	Records Mgt. Official
1E	Laws and Regulations	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓						
2.1E	SP – Planning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓				
2.2E	SP – Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓					
3.1E	SLCS – Initiation		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓			✓			
3.2E	SLCS – Development							✓	✓	✓	✓		✓	✓	✓	✓	✓				✓	✓	✓	
3.3E	SLCS – Test & Evaluation			✓	✓	✓			✓	✓	✓		✓	✓	✓	✓	✓		✓		✓		✓	
3.4E	SLCS – Implementation			✓	✓		✓		✓	✓	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓	
3.5E	SLCS – Operation							✓		✓	✓	✓	✓	✓	✓	✓	✓						✓	
3.6E	SLCS – Termination	✓				✓	✓	✓						✓	✓	✓		✓						✓
Key:	SP = Security Program SLCS = Sys Life Cycle Security																							

Use Role



		Core Body of Knowledge												Position			
Cell	Domains	Laws and Regulations	IT Security Program	System Environment	System Interconnection	Information Sharing	Sensitivity	Risk Management	Management Controls	Life Cycle Controls	Operational Controls	Awareness and Training	Technical Controls	ISO/ISM	Users	System Owner	Info. Resource Manager
1F	Laws and Regulations	✓							✓			✓		✓	✓	✓	✓
NA	SP – Planning																
NA	SP – Management																
3.1E	SLCS – Initiation		✓				✓	✓						✓	✓	✓	
3.2E	SLCS – Development						✓		✓					✓	✓		
3.3E	SLCS – Test & Evaluation								✓		✓			✓	✓	✓	
3.4E	SLCS – Implementation						✓		✓					✓	✓		
3.5E	SLCS – Operation								✓		✓	✓	✓	✓	✓		
NA	SLCS – Termination																
Key:	SP = Security Program SLCS = Sys Life Cycle Security																