Information System Life Cycle Development Category and Component Security Methodology

Created by Martin Connell, *Information Security Specialist*

www.martinconnell.com

B.S. Information Technology Security from Western Governors University

CompTIA Security + CompTIA Network + CompTIA Project + CompTIA A+ Technician

Sun Java Associate CIW Professional CIW Database Design Specialist

Microsoft 70-270 Windows XP - Configuration, Installation & Maintenance
Microsoft 70-298 Designing Security for a Windows 2003 Server Network

Contents

Introduction

As cyber security is becoming an increasing concern for organizations, much focus has been placed on creating new or better Information Technology Security appliances or architectures such as vulnerability scanners and Zero Trust/Application Centric Infrastructure (ACI) networks. However, the root cause of many information system vulnerabilities can still be traced back to poor life cycle development processes and procedures that allowed systems with inadequate security controls and/or poor designs to be placed into the production environment in the first place. While new processes and applications have been developed to assist organizations to manage governance, risk and compliance (GRC) responsibilities in order to protect the organization's information and information systems, very little has been created to offer a consistent process for information system life cycle development security. Even NIST 800-64, National Institute of Standards and Technology guidance for secure information systems life cycle development for Federal agencies, does not provide concrete processes or procedures for ensuring information systems are developed and produced with adequate security controls to limit potential vulnerabilities.

The Information System Life Cycle Development Category and Component Security Methodology (ISLCD-CCSM) was developed to address deficiencies within the information system life cycle development process pertaining to security controls. The ISLCD-CCSM is intended to interject the role of information security as an integral part of the life cycle with disciplined and enforceable processes. While organizations have focused more resources on the auditing of existing information systems for security controls compliance, applications have been created to assist with the process and ensure accountability. However, little exists to track security compliance within the life cycle development process. With the introduction of the Information System Life Cycle Development Category and Component Security Methodology, applications may also be created to assist Information Security Specialists with information system life cycle development security to ensure consistent and auditable processes.

The key to the Information System Life Cycle Development Category and Component Security Methodology (ISLCD-CCSM) is to compartmentalize the purpose(s) of the information system and its corresponding system components. First, the purpose(s) of the information system is categorized (data integration, data analytics, application implementation, application development, etc.) and then the components of the information system such as application software, system software, computing hardware and nodes can be identified for each category. This allows Information Security Specialists to create a detailed Security Plan for the information system consisting of specific security controls expected to be implemented for the components at the beginning of the development process as recommended by NIST 800-64. The Security Plan will be essential for providing Project Managers, architects and developers with the controls that must be included in the design and implementation of the information

system. With the Security Plan in place, a disciplined and enforceable process can be implemented to ensure the security controls are included and correctly implemented throughout the process. This process will also help reduce issues related to scope creep as to where any requirements (categories) or components added to the information system during the process can be identified by the Information Security Specialist and additional controls can be added to the Security Plan as needed. By implementing the ISLCD-CCSM, vulnerabilities and risks to the organization can be reduced and incorporating proper change management procedures throughout the production cycle of the information system, fewer resources will be required to deal with audit remediation in the long term.

Category and Component Methodology for Securing Information Systems

One of the most difficult challenges for Information Security Managers is to clearly identify information systems' risks because of the number and complexity of the information systems within the organization. The ISLCD-CCSM proposes a clear strategy for identifying and organizing potential risks by using a system category and component based methodology for assessing risks and applying security controls. The ISLCD-CCSM defines an information systems as:

> **Information System:** an integrated set of computer components, both hardware and software, for collecting, storing and processing data and for providing information and/or performing a task.

Information System Category

In order to properly compartmentalize an information system, it is critical to identify its purpose(s). The purpose(s) of the systems directly corresponds with stakeholders' requirements to perform some type of task(s) or function(s). This is generally determined during the Request for Proposal (RFP) process for most organizations, but requirements may be added during the development life cycle process as a result of scope creep. In order to clearly identify and organize these purposes for applying security controls, these purposes (tasks/functions) are placed into a specifically defined category. An information system may be composed of many types of specific categories. The following is a list of most applicable categories for an information system:

- Data Integration
- Data Extraction
- Data Transport
- Data Storage

- Data Analysis
- Data Processing (Calculations)
- Mechanical/Robotics
- Application Implementation
- Application Development

Information System Component

Once a category of an information system has been identified, the corresponding components required for the category can be identified. The following are the four components of an information system:

1. **Application Software** – a computer program designed to perform a group of coordinated functions, tasks or activities for the benefit of the user. Examples include but are not limited to: database programs, email clients, word processors, spreadsheets, Web browsers and plug-ins, games and calculation programs.
2. **System Software** – a type of computer program that is designed to run a computer's hardware and application programs and includes operating systems, compilers and utilities for managing computer resources. Examples include but are not limited to: Microsoft Windows/Server, Unix OS, Java runtime environment, C++ compilers and device drivers.
3. **Computing Hardware** – physical computing device(s) required for software to operate and function. (i.e. PC's, laptops, servers, tablets, smart-phones, etc.)
4. **Nodes** – Special networking, storage, security, input/output and other devices required for the information systems to function. (i.e. switches, Storage Area Networks, firewalls, load balancers, printers, robotic arms, electronic locking mechanisms, etc.)

Securing Information System Components

The purpose of categorization is to identify relevant system components and the purpose of identifying system components is to identify the risks within each component. By identifying potential risks within a component, security controls can be applied to minimize those risks. Security controls may be based on the organization's information security standards and policies and may include specific baselines based on industry or regulatory standards such as NIST- FISMA, PCI, HITECH, HITRUST, etc. Information Security Specialists can identify and document these required controls at the beginning of the development process and routinely assess the design and implementation of the controls throughout the life cycle development process.

Applying Security Controls throughout the Information System Development Life Cycle

The purpose of the Information System Life Cycle Development Category and Component Security Methodology (ISLCD-CCSM) is to ensure that proper security controls are applied to an information system to minimize risks and vulnerabilities posed by the system. The primary objective is to ensure that risks are minimized as much as possible before the system is placed into production. The ISLCD-CCSM also addresses the minimization of risks throughout the entire system life cycle too including proper change management processes during production, routine security audits during production and proper decommission of system components post production. By applying standard processes as proposed by the ISLCD-CCSM, the objective of minimizing risk from the information system throughout the entire life cycle can be achieved consistently throughout the organization by providing a disciplined, enforceable and accountable methodology.

Information System Security Plan

The Information System Security Plan is created by the Information System Life Cycle Development Information Security Manager (ISM) during the beginning phase of the development process. Once the requirements for the information system have been determined during the Requirements phase (usually during a Request for Proposal), enough information should be documented in an initial project plan to determine the information system's categories. From there, the category components can be either determined or inferred.

Determined Information System Components – during the requirement phase, a system architect has clearly defined a solution for the requirements including specific components such as required application software, system software, computing hardware, nodes and vendors. As a result the ISM can create a specific list of security controls to be implemented for the components. In this scenario, the only changes to the Security Plan will be made if components are changed or added during the information system's life cycle.

Inferred Information System Components - during the requirements phase, a system architect has not provided specific solutions for the information system; rather, only general system specifications are provided. This scenario may include the vetting of potential vendors or the need for further research to determine specific application software, system software, computing hardware or node types. As a result, the ISM will create a general Security Plan based on general component types that may be inferred from the categories. In this case, the

Security Plan will list general security controls that will be expected no matter the specific component solution such as role based access controls, password requirements, system software baselines, port rules, vendor qualifications, etc. This information can then be used as a guide by the Project Manager, system architects and developers when researching and determining specific component solutions. Once a component solution has been determined and approved by the ISM based on the ability to conform to required security controls, the component will then be classified as a Determined Information System Component and the ISM will update the Security Plan with controls specific to that component.

Information System Security Plan Maturity

As the information system components are developed and tested, the Security Plan may be changed or amended to reflect changing or additional components. For some types of components such as newly developed application software, additional security controls may be added by the ISM during the development phase as a result of idiosyncrasies found with a particular component such as a programming language or application server or as a result of additional risks discovered during testing phases.

During the production cycle of the information system, changes or amendments to the Security Plan may be made to reflect changes made to components such as upgrades, releases, patches or additional components all together. Any changes made to production information system components should be implemented through a strict change management control process to include testing and certification of affected components. Changes made to the Security Plan should be seamlessly incorporated into the change management process with complete involvement and approval of the ISM.

The Security Pan may also be changed or amended as a result of any deficiencies found by routine security audits of system components. During the decommissioning of an information system and its components, the Security Plan should also be amended and enforced through a strict change management process to address security controls and procedures required to decommission components in accordance with the organization's security standards and policies.

It is recommended that all changes and amendments of the Information Security Plan be versioned so that the history of changes can be easily ascertained and those responsible for changes can be accountable. An application with the ability to version documents as part of the life cycle documentation process would be desirable and be a standard requirement for any application designed for implementing the Information System Life Cycle Development Category and Component Security Methodology. Such as system would allow the organization's

managers, auditors and regulators to review the complete life cycle history of an information system and prove due diligence of applying security controls for the information system throughout its history from development through decommission.

The Information System Life Cycle Development Category and Component Security Methodology Process

Although life cycle development process may differ from one organization to another, the following process is recommended based on NIST 800-64 guidelines for information systems life cycle development security:

Requirements Phase Information Security Plan Questionnaire

The process of gathering requirement for an information system may differ among organizations and even within organizations based on capital requirements. In some cases a formal committee approach may be implemented to create a Request for Proposal (RFP) or a project may be initiated by a department(s) based on a specific need(s). In either case, it is recommended that an Information Security Specialist be involved in the requirements gathering process as much as possible whether during the RFP process or by reviewing Business Requirements Documents. However, this may not be possible or practical for some organizations.

As part of the ISLCD-CCSM, though, the Information Security Manager (ISM) for the information system must be consulted after the requirements have been determined and before the design phase begins. The ISM shall provide relevant stakeholders, usually the system architect or Project Manager, a Security Plan Questionnaire to determine the information system's categories and components. The information provided will then be used to create the initial Information System Security Plan. The Security Plan will be published for all relevant stakeholders to access to ensure everyone involved is aware of the security controls required for design and implementation of system components. If the life cycle project follows a process of reviewing and amending Business Requirements Documents (BRD), the ISM will review all such documents to determine if categories and components have been changed or added and update the Security Plan accordingly. This may include additional Security Plan Questionnaires during the requirements phase to better identify such changes. The redundancy of several questionnaires will also help identify any errors made by stakeholders when first identifying categories and components.

A centralized application could be used to provide and track the Security Plan Questionnaires to relevant stakeholders and to publish the resulting Security Plan for role based access. This

would provide and enforceable and auditable trail of documentation regarding the life cycle development process and validate due diligence to reduce risks.

Design Security Plan Implementation Processes

As functional and technical documents are provided by stakeholders such as architects and developers during the design process, the ISM will be responsible for reviewing specifications and designs to ensure proper security controls listed in the Information System Security Plan are included for each component. This is accomplished by collecting evidence of compliance with security controls documented in the Security Plan by the Information Security Manager (ISM) from relevant stakeholders such as Project Managers, system architects and developers. The ISM or a team of Information Security Specialists shall be responsible for verifying the supplied evidence as being valid and sufficient to meet security controls. This process continues throughout the design and testing processes of system components. The following are types of evidence that can be used to determine compliance with required security controls for system components:

Screen Shots – stakeholders may provide screen shots of security controls being applied to a component such as:

- Role based access permissions settings
- Configurations of passwords and access settings
- Node configuration settings
- System software configurations
- Vendor agreements
- Code base examples
- SQL statements and table examples

Reports – stakeholders may provide reports documenting compliance with security controls or proving that risks have been resolved. Such reports may include:

- Static code analysis of application software
- Dynamic code analysis of application software
- Vulnerability testing report
- Vendor assessment report
- Independent industry compliance report

Attestation Statements of Compliance – certain stakeholders or officials may provide statements attesting that certain security controls have been verified. This includes attestations

from Information Security Specialists that have witnessed compliance or verified compliance through hands-on experience with the component.

Security Questionnaires – Additional questionnaires may be completed by stakeholders to ensure component security controls are being addressed throughout the design and testing process and to help identify any changes made to components or components added since the requirements phase (scope creep). Security questionnaires should be:

- Short and precise
- Only relevant for the specific component
- Understandable by stakeholders involved
- Designed so that answers may be easily scored and analyzed by the ISM

A centralized application could be used to provide and track security controls evidence and provide questionnaires to relevant stakeholders and to publish the results for role based access. This would provide and enforceable and auditable trail of documentation regarding the life cycle development process and validate due diligence to reduce risks by verifying controls compliance within a central repository.

Implementing Security Plan in a Matrix Environment

In project management environments such as Scrum/Agile derivatives, implementing security controls for components will follow the design process. Evidence for security controls compliance will be provided during each iteration of the design and testing phase. This may include code analysis and vulnerability testing during each iteration, especially for application software components. In addition to evidence collected during iterations, evidence should also be provided during User Acceptance Testing of the entire information system. This is to ensure that once the system components are assembled, the entire system functions properly, which should be a security requirement.

Inadequate Security Controls Enforcement Process

If stated security controls are not implemented for components during the design and testing process, The ISM will create a deficiency finding for the component similar to an audit finding. The Project Manager for the information system development project will be responsible for coordinating finding responses and remediation. It may or may not be possible for the design and testing process to move forward until a deficiency is remedied depending on the finding and component type. It will be up to the ISM and Project Manager to make this determination

on a case-by-case basis. Once evidence has been supplied and approved to remedy the finding, the ISM will clear the finding as satisfied.

It is advisable that all deficiency findings be recorded and retained in some type of application or data repository for future reference. A documented history of findings and remedies can be very useful for future system audits or for troubleshooting.

Information System Pre-Production Certification

As security controls for the information system's components are satisfied during the design and testing processes, the information system will be certified to go into production. This is considered a "pre-production" certification because the information system needs to be monitored for a period of time after being placed into production for any issues or risks not discovered during testing. To pre-certify the system, the ISM will conduct a review of all security controls listed in the Information System Security Plan and the evidence received for compliance. In some cases, a Senior Information Security Specialist or a team of Information Security Specialist may review and verify that all controls have been satisfied. Upon approval, the information system will be officially "pre-certified" and cleared to enter into production.

Information System Production Certification

After the information system is placed into production it should be closely monitored for a period of time to be determined by the ISM and relevant stakeholders. The monitoring period will be based on component types, the importance of the information system and other variables determined by stakeholders. Once the initial monitoring period has expired with no detected issues or risks, the ISM will then officially certify the information system as a "Production System."

After the system has been certified for production, components should still be monitored throughout the production life cycle. If an issue is detected or encountered during production, the production certification will be suspended until remedies are applied and approved by the ISM and relevant stakeholders. Depending on the issue(s) the information system may or may not remain in production until remediation is satisfied. If it is deemed the system can stay in production during remediation, the affected system components should be closely monitored and once the remedy has been applied and verified, the system will be re-certified as a production system. If the system needs to be taken out of production to apply remedies, the components will go through the design and testing cycle and then go through the pre-production certification and production certification processes.

Routine Information System Security Audits and Re-Certification

As part of the production life cycle process, the information system and its components should undergo routine audits for compliance. The audit should determine that all security controls for components listed in the Information System Security Plan are implemented. The purpose of the audit is to discover the following issues:

- Security controls have been disabled or removed
- Existing security controls have become deprecated or inadequate
- Unauthorized changes have been made to security controls or affected configurations
- Unauthorized components added to the information system
- Unauthorized removal of information system components
- Failure to properly monitor components
- Unusual or frequent component malfunctions or failures
- Issues with vendors or changes with vendors

After successful completion of the audit, the ISM will re-certify the information system as a Production System. If the audit results in findings, the information system or its affected components may have to go through the pre-certification and production certification process again.

Information System Decommission Certification

At the end of the information system's production cycle, components will need to be properly decommissioned once taken out of production. Decommission may include removal of sensitive data, removal and archival of application software, destruction of hardware and drives, reset of nodes, etc. The information System Security Plan will be amended during the decommission phase to include all of the necessary tasks required by the organization's security standards and policies to properly decommission each component. Evidence will be collected and documented verifying that all decommission tasks have been completed and verified. The ISM and/or a Senior Information Security Specialist or a team of Information Security Specialist will review the evidence and certify the information system as decommissioned.