Information Systems Component-based Security Assessment 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

Information Systems Component-based Security Assessment Methodology Introduction

The objective of the Information Systems Component-based Security Assessment Methodology (ISCBSAM) is to provide a consistent and disciplined method for assessing large and complex information systems for security controls compliance. Security controls and standards may vary from one organization to another based on individual needs and management philosophies, but the methodology for assessing the information systems should be the same regardless of the individual controls being examined. The challenge for evaluating information systems is relevant to the size and complexity of the systems. While security controls objectives such as those documented by NIST and ISO are widely accepted and utilized by many organizations, the procedures and methods for organizing, prioritizing and assessing individual information systems for compliance are usually left up to the individual organization or auditors. Therefore, the Information Systems Component-based Security Assessment Methodology has been designed to give organizations and auditors a standard methodology for assessing information systems and to compliment standards such as NIST and ISO 2700. This methodology can also be utilized for assessing information systems for industry specific standards such as PCI and HIPPA. The goal of the ISCBSAM is to save organizations time and money assessing information systems by better organizing resources while at the same time achieving greater security of the organization's information and systems.

Defining an Information System

The most critical aspect of the Information Systems Component-based Security Assessment Methodology is to clearly define an information system and its components, hence the term "component-based." By defining the components of an information system, a disciplined approach to organizing, prioritizing and assessing the components for security compliance may be achieved and applied consistently throughout an organization.

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. An Information System consists of the following components:

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.)

Methodology – Identify, Organize, Prioritize and Assess

The purpose of the Information Systems Component-based Security Assessment Methodology is to provide a simple and consistent approach for evaluating the security controls of any type of information system regardless of size and complexity. This is achieved by utilizing the component-based approach to identifying the parts of the information system. The following are the four primary elements of the ISCBSAM:

Identify

The most critical element of the ISCBSAM is to clearly identify the following aspects of an information system:

- Each component of the system (application software, system software, computing hardware and nodes)
- The types of information contained in, processed by or touched by each component
- The overall purpose of the information system and its components
- The criticality of the information system and its components to the organization

Organize

After the components, information types, purpose(s) and criticality of the information system have been identified, they should be organized into specific categorized based on the following:

Component Types and Classifications – After the general type of each component within the information system has been identified, it can then be organized into more specific categories. The following are specific categories types that may be utilized in organizing system components:

I. Application Software

A. Software Type

- Software as a Service (SaaS)

- Commercial Off-the-Shelf (COTS) Application
- Internally Developed Application
- Third-Party Developed Application
- Internal and Third-Party Collaborative Development Type Application

B. Application Purpose(s)

- Database
- Data Analytics
- Data calculations and processing
- Gaming and Entertainment
- Data input or output interface
- Data transportation and/or management
- Protection (anti-malware)
- Mechanical controls

II. System Software

A. Software Type

- Operating System
- Utility
- Program language compiler or environment
- Device Drivers

III. Computing Hardware

- PC
- Laptop
- Server
- Tablet
- Phone
- Industry Specific Computer

IV. Nodes

A. Node Types

- Switches
- Firewalls
- Load Balancers
- Printer/Scanners/Copiers
- Storage Devices
- Cameras
- Mechanical Devices (i.e. door locks, robotic arms, etc.)
- Bar code readers
- Industry Specific Devices

B. Node Purpose
    - Network Traffic Routing
    - Network Traffic Protection
    - Storage
    - Data Output
    - Data Input
    - Physical Actions
    - Protection – Surveillance

Information Types and Classification – After the types of information contained in, processed by or touched by each component have been identified, they should be categorized based on the following:

- Organization's Information Classification Levels (i.e. Restricted, Confidential, Sensitive, Public, etc.)
- Industry Specific Classifications (PHI, PII, PCI, FISMA, etc.)
- Importance of Information for Business Operations

The recommended approach for scalable organization of information categorization for future prioritization would be to assign one of the following labels to the information type:

Critical – loss or compromise of the information would subject the organization to significant adverse actions (publicity, fines, litigation, etc.) from outside organizations, parties and/or government agencies.

Important – loss or compromise of the information would have adverse consequences to the organization, but not necessarily subject the organization to actions from outside organizations, parties or government agencies.

High – the information is considered sensitive to the organization, but not rising to the higher levels of confidentiality or restrictions.

Medium – the information is considered sensitive for internal use by the organization, but loss or compromise would not have an overall significant impact on the organization.

Low – the information is regarded as public or public domain and has no sensitive value for the organization.

Categorize Criticality of Information Systems – It is important to clearly categorize how important an information system is for the organization and its operations. Some systems may

not necessarily be required to perform business functions, but may be critical for regulatory compliance operations or for contractual compliance obligations. The following scale is based on a system's required return to operations status in the event of a failure or malfunction:

Critical – the system must be operational at all times and any failure or malfunction would have an immediate negative impact on the organization. Return to Operation (RTO) = less than 24 hours.

Important – the system has the second highest RTO priority other than those that are deemed Critical. RTO = within 24 hours.

High – the system can only be non-operational for a limited time before having a negative impact on the organization. RTO = within 24 to 48 hours

Medium – the system is important for the organization, but can be non-operational for a significant time before having a negative impact on the organization. RTO = 48 to 72 hours.

Low – failure of the system will not have any significant impact on the organization. RTO = 72 hours or more.

Prioritize

After component types, information types and criticality of systems have been organized, they can then be prioritized for assessment. While prioritization specifications can vary from one organization to another, the Information Systems Component-based Security Assessment Methodology provides for an objective structure for prioritizing the assessments of components.

Component Prioritization Table Scale - by applying the following scale, organizations can better determine the order in which to assess information system components and how to devote available resources for such assessments:

Criticality Level

Information Level	Critical	Important	High	Medium	Low
Critical					
Important					
High					
Medium					
Low					

To use the scale, place the component in the appropriate box based on its assigned Information Level and Criticality Level. Example:

Criticality Level

Information Level	Critical	Important	High	Medium	Low
Critical	SQL Server		Billing App		
Important			Web Application		
High		Access db			
Medium					
Low	Website				

Once the component has been placed in the appropriate Prioritization sector within the scale, components can then be further prioritized by those touching or applying to the most number of information systems. For example: some components such as a SQL Server may be used by several applications touching various levels of information with varying degrees of criticality. In this case, the component will be assigned the highest level of information it touches and the highest level of criticality based on the other information systems it touches.

Component Prioritization Formula - a numerical formula for prioritization may also be used by assigning a number value to each scale:

Information and Criticality Level	Prioritization Number
Critical	5
Important	4
High	3
Medium	2
Low	1

Based on assigned Prioritization Numbers, the following formula can be used to prioritize components for assessment:

(*Information Level*) x (*Criticality Level*) + (*Number of Information Systems Touched*)

In the following example, a SQL Server Application (application software component) that touches 3 information systems has an Information Level of 5 and a Criticality Level of 4:

(*Information Level = 5*) x (*Criticality Level = 4*) + (*Number of Information Systems Touched = 3*)

The Priority Rating for the component = 23

Prioritization Scale and Formula Hybrid - by combining the Prioritization Table Scale with the Prioritization Formula, organization Information Security managers can provide an objective overview for prioritizing assessments and required resources for the assessments. While most organizations' managers will eventually have to make some subjective judgments as to exactly which components to prioritize based on resources and other variables, the process to make a final decisions will be greatly enhanced and expedited by applying the Information Systems Component-based Security Assessment Priority Methodology. The example below utilizes both the Prioritization table scale and the Prioritization Formula for creating an assessment priority overview of information system components:

Criticality Level

Information Level	Critical	Important	High	Medium	Low
Critical	SQL Server 23		Billing App 16		
Important			Web Application 13		
High		Access db 13			
Medium					
Low	Website 8				

Assessment – Component-based Resource Assessment Methodology

By applying the Information Systems Component-based Security Assessment Methodology (ISCBSAM) principles to identifying, organizing and prioritizing components, the assessment process can be executed efficiently and effectively by utilizing only those resources required to perform assessment evaluations for a particular component. Rather than having a single Information Security Auditor attempt to evaluate and assess a multitude of component types within a given information system, requiring an extensively broad and yet refined skill set and knowledge base, information system audits can be performed by multiple Information Security professionals with each specializing in specific component areas. By utilizing the ISCBSAM, the Information Security Auditor performs the role of an Information Security Assessment Project Manager (ISA-PM) and utilizes other Information Security professionals as resources for completing the assessment. Dedicated team members perform detailed assessments specifically for components for which he/she is qualified based on one's skill set, knowledge base and experience. This greatly reduces the struggle for management to recruit individuals with such skills and experience that make them difficult to find and even harder to retain. By employing a "team approach" to information security assessment/audits, it is much easier to recruit and retain individuals with more niche skills and experience. The ISCBSAM "security team approach" also makes it much easier for management to outsource particular members of

the assessment/audit team as needed. For example, a software penetration specialist can be contracted to help assess components that are classified as internally developed application software.

Information Systems Component-based Security Assessment Team

Although every organization is different and assessment situations are unique to the organization, a general recommendation can be provided for the structure of an Information Systems Component-based Security Assessment Team. In many cases, some team members will fill several roles based on his/her skills and experience. Cross domain training for team members is also highly encouraged whenever possible within the organization. The following takes into account the use of all potential information system components required to be assessed:

Chief Information Systems Security Assessment Officer (CISSAO) – this is the primary party responsible for identifying all relevant information systems for assessment. The CISSAO leads and manages the overall Information Systems Component-based Security Assessment Team and is responsible for the overall identification, prioritization and assessment of all relevant information system components.

Security Assessment Project Manager (ISA-PM) – this is the primary party responsible for managing the identification, organization, prioritization and assessment of components within an information system. The ISA-PM is responsible for leading and managing other team members to perform assessments for each component.

Application Software Security Assessment Specialist (ASSAS) – this party provides assessment for application software components and may be compromised of several specialists based on the categorization of the application software:

- Software as a Service Application Assessment Specialist
- Specific Programming Language(s) Security Specialist
- Database Application(s) Security Specialist
- Software Application Penetration Specialist
- Commercial Off-the-Shelf (COTS) Application Security Specialist

System Software Security Assessment Specialist (SSSAS) – this party provides assessment for system software components and may be compromised of several specialists based on the categorization of the system software:

- Operating System Specific Security Specialist
- Utility Specific Security Specialist

- Language or Software Platform Specific Security Specialist (Compilers, runtime environments, etc.)

Computing Hardware Security Assessment Specialist (CHSAS) – this is the primary party responsible for assessing computing hardware such as servers, PC's, laptops, tablets, smart phones, etc.

Node Security Assessment Specialist (NSAS) – this party is responsible for assessing node hardware and software systems specific for the node, which is considered proprietary for the node's operation and not considered to be a separate system or application software component. Because of the vast number of node types, a NSAS may specialize in a particular node type or types such as switches, firewalls, SAN's, printers, robotics, etc.

Vendor Security Assessment Specialist (VSAS) – this party performs assessments for vendors that provide information system related components or services. There may be several VASAS based on specific types of components, systems and services being provided and assessed.

Information Systems Component-based Security Assessment Team Advantages

The advantages for organizations to employ the Information Systems Component-based Security Assessment Team Methodology are:

Scalability – using the component-based team methodology for performing information system security assessments allows organizations to evaluate large numbers of complex information systems within the organization. The granularity of the component-based approach allows organizations to more easily identify and apply resources for assessments than other traditional or less organized assessment methods.

Efficiency – by having specific team members assess components individually, more work is accomplished simultaneously for completing overall information systems assessments. This results in more assessments being performed in shorter periods of time than those performed using traditional or less organized methods.

Quality – by having professionals with specific skills and experience focus on relevant information system components, security assessments will be more thorough and issues will be less likely overlooked than with assessments performed using traditional or less organized methods.