SECURE CODE ALLIANCE PRACTITIONER (SCA PRACTITIONER) TRAINING SYLLABUS

version 2025.2

PUBLIC

Public Release Authorized

Table of Contents

SECURE CODE ALLIANCE (SCA) ECOSYSTEM OVERVIEW

The Secure Code Alliance (SCA) is focused on technical competence of both individuals and organizations that develop Applications, Services and Processes (ASP). With evolving statutory and regulatory requirements mandating Secure Development Practices (SDP), the SCA is uniquely situated to assist with evidence to demonstrate familiarity with and a commitment to SDP at the:

- Individual-level; and
- Organization-level.

INDIVIDUAL-LEVEL

The SCA expects developers to invest the requisite time and effort necessary to familiarize themselves with referenced materials, since these voluntary consensus standards form the basis of the SCA Body of Knowledge (SCA-BoK) that is leveraged in the conformity assessment.[1]

The SCF Assessor and Instructor Certification Organization (SAICO) is authorized by the SCA to conduct individual-level certification-related services for the:

1. Certified SCA Practitioner (CSCAP) - "practitioner-level competency" among developers; and
2. Certified SCA Architect (CSCAA) – "expert-level competency" among architects.

PRACTITIONER ROLE - CERTIFIED SCA PRACTITIONER (CSCAP)

Application developers (practitioners) are expected to use Software Development Life Cycle (SDLC) processes for new systems, system upgrades, or systems that are being repurposed. These processes can be employed at any stage of the system lifecycle and can take advantage of any system or software development methodology, including agile, spiral, or waterfall.

CSCAPs are expected to:

- Apply lifecycle processes recursively, iteratively, concurrently, sequentially, or in parallel and to any system regardless of its size, complexity, purpose, scope, environment of operation, or special nature.
- Understand and operationalize the organization's security architecture that must be followed for application development processes for development, testing, staging and production environments.
- Incorporate the organization's risk management practices throughout application development processes across the entire SDLC.
- Develop software applications in accordance with industry-recognized secure coding practices.
- Incorporate security and privacy measures throughout the SDLC.
- Control changes to ASP across the SDLC using formal change control procedures.
- Review custom code through a formal change management and approval process prior to release to production.
- Remove custom application accounts, user IDs and passwords before applications become active or are released to customers.
- Confidently review SBOM documentation for security and privacy-related implications.
- Perform software conformity assessments.

ARCHITECT ROLE - CERTIFIED SCA ARCHITECT (CSCAA)

Architects are expected to employ cyber resiliency constructs (e.g., goals, objectives, techniques, approaches and design principles), as well as the analytic and lifecycle processes, to tailor them to the technical, operational and threat environments for which the architect's systems need to be engineered.

CSCAAs are expected to:

- Define the security architecture(s) the organization will follow for application development processes.
- Define application development considerations for the organization's risk management practices across the entire SDLC.

---

[1] *SCA BoK - https://securecodealliance.com/sca-bok/*

- Publish rules for the organization's application development processes for development, testing, staging and production environments.
- Develop conformity assessment practices for the organization to follow in order to demonstrate alignment with stated Secure Software Development Practices.
- Ensure that information security and privacy principles are an integral part of Secure Software Development Practices (SSDP) across the entire SDLC.
- Ensure security & privacy-related measures are included in the requirements for new systems or enhancements to existing systems.
- Ensure application development practices (internal and external) adhere to industry-recognized secure coding practices.
- Develop Software Bill of Materials (SBOM) documentation for application development projects.
- Oversee changes to ASP across the SDLC using formal change control procedures.
- Oversee application security testing practices.
- Implement the SSDP concepts and techniques for all High Value Assets (HVA):
    - New Systems;
    - Dedicated or Special-Purpose Systems;
    - System of Systems;
    - System Modifications;
    - System Evolution; and
    - System Retirement.

ORGANIZATION-LEVEL

There are two (2) types of organization-level offerings:

1. Secure Development Organization (SDO) designation; and
2. Certified Organization for Development Excellence (CODE) certification.

The Cyber AB governs organization-level SCA designations and certifications.[2]

SECURE DEVELOPMENT ORGANIZATION (SDO)

The SDO designation was developed as a way for organizations to clearly identify a commitment to SDP, through:

1. Adherence to the respective requirements and constructs of the SCA framework; and
2. Employing SCA-certified individuals to operationalize SDP.

There are three (3) levels of SDO:

1. **SDO**
    a. Organization is registered with the Cyber AB as a SDO; and
    b. Employs at least one (1) CSCAP.
2. **SDO Advanced**
    a. Organization is registered with the Cyber AB as a SDO; and
    b. Employs at least three (3) CSCAP.
3. **SDO Elite**
    a. Organization is registered with the Cyber AB as a SDO; and
    b. Employees at least:
        i. Three (3) CSCAP; and
        ii. One (1) CSCAA.

CERTIFIED ORGANIZATION FOR DEVELOPMENT EXCELLENCE (CODE)

The concept of the Certified Organization for Development Excellence (CODE) certification is to utilize a third-party conformity assessment of SDP. CODE certification is exclusive of a SDO designation, where an organization does not have to be a SDO to seek/obtain CODE certification.

[2] *The Cyber AB - https://cyberab.org/*

For CODE, the SCA:

- Appointed The Cyber AB to serve as the Accreditation Body (AB) for the SCA's organization-level certification scheme; and
- Leverages the Secure Controls Framework Conformity Assessment Program (SCF CAP) for the methodology and infrastructure to conduct the conformity assessment.[3]

As part of the SCF CAP, an Organization Seeking Assessment (OSA) hires a SCF Third-Party Assessment Organization (SCF 3PAO) to perform Third-Party Assessment, Attestation & Certification (3PAAC) services.

There are three (3) CODE levels that are designed to be progressive, building upon the previous CODE level:

1. **SCF Certified - SCA CODE 1**
    a. Focus: Organization-level attestation of SDP.
    b. Control Set: The CISA Secure Software Development Attestation Form (SSDAF) is used as the basis for CODE 1 certification.[4] CISA derived the SSDAF directly from the requirements outlined in Executive Order (EO) 14028.[5]
    c. Prerequisite(s): None
2. **SCF Certified - SCA CODE 2**
    a. Focus: Commercial Off The Shelf (COTS) Applications, Services and Processes (ASP)
    b. Control Set: NIST SP 800-218, Secure Software Development Framework (SSDF).[6]
    c. Prerequisite(s): SCA CODE 1 (may be conducted in conjunction with SCA CODE 1)
3. **SCF Certified - SCA CODE 3**
    a. Focus: Custom ASP
    b. Control Set: Tailored SCF control set (bespoke for the specific use case).
    c. Prerequisite(s): SCA CODE 2

[3] *SCF CAP - https://securecontrolsframework.com/certification/scf-conformity-assessment-program-cap/*
[4] *CISA Secure Software Development Attestation Form - https://www.cisa.gov/secure-software-attestation-form*
[5] *EO 14028 - https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity*
[6] *NIST SP 800-218 - https://csrc.nist.gov/pubs/sp/800/218/final*

Secure Code Alliance Practitioner (SCA Practitioner) Training Overview

Course Title
Secure Code Alliance Practitioner (SCA Practitioner) Training

Online Course Access
Students have one hundred eighty (180) days from the date of purchase to complete SCA Practitioner training before the student is disenrolled and access is revoked.

Course Cost & Certification Lifecycle
The Certified SCA Practitioner (CSCAP) certification is valid for a duration of three (3) years from issuance, at which point the certificate must be renewed or it is expired.

The table below shows:
(1) Initial training and certification cost; and
(2) If necessary for retaking the knowledge exam, a knowledge exam license.

Description	Course Fee (one time)
SCA Practitioner Training	$350
Knowledge Exam License (retakes)	$100

The CSCAP certification is valid for three (3) years from the date of issuance until it expires. There is no ongoing certificate maintenance. Upon expiration, individuals will be required to retake the SCA Practitioner Training course to enhance their knowledge with current secure coding practices.

If there is a major change in coding standards and practices, they will be addressed in the next iteration of the course. When the course is updated with these new practices, SCA Practitioners will be notified via email regarding this major update.

Course Registration
Prospective students can sign up for SCA Practitioner training online at:
https://training.securecontrolsframework.com/products/courses/sca-practitioner

Language Specification
SAICO-provided training and knowledge exams are currently only available in English.

Number of Credit Hours
Students should expect to spend at least eight (8) hours to complete the CSCAP training, including reading the documents identified as prerequisite reading materials.

Course Description
CSCAPs are SAICO-certified individuals who have the knowledge and skills to:
(1) Apply lifecycle processes recursively, iteratively, concurrently, sequentially, or in parallel and to any system regardless of its size, complexity, purpose, scope, environment of operation, or special nature.
(2) Understand and operationalize the organization's security architecture that must be followed for application development processes for development, testing, staging and production environments.
(3) Incorporate the organization's risk management practices throughout application development processes across the entire SDLC.
(4) Develop software applications in accordance with industry-recognized secure coding practices.
(5) Incorporate security and privacy measures throughout the SDLC.
(6) Control changes to ASP across the SDLC using formal change control procedures.

(7) Review custom code through a formal change management and approval process prior to release to production.
(8) Remove custom application accounts, user IDs and passwords before applications become active or are released to customers.
(9) Confidently review Software Bill of Materials (SBOM) documentation for security and privacy-related implications.
(10) Perform software conformity assessments.

PREREQUISITES:
While there are no formal educational or certification prerequisites to become a CSCAP, to successfully pass the knowledge exam and perform duties as a CSCAP, students are expected to have:

(1) Six (6) months, or more, of practical experience with the Secure Development Practices (SDP);
(2) Familiarity with the following publications / resources:
   a. Executive Order (EO) 14028;[7]
   b. NIST SP 800-218 v1.1; [8]
   c. NIST SP 800-218A;[9]
   d. NIST SP 800-160 (vol 1 & 2); [10]
   e. OWASP Top Ten; [11]
   f. SCA Body of Knowledge;[12] and
   g. SCA's Code of Professional Conduct (CoPC).[13]

COURSE LEARNING OUTCOMES
After successful completion of this course and earning the CSCAP designation, students are expected to be conversational on the following topics:

(1) What constitutes industry-recognized Secure Development Practices (SDP);
(2) How EO 14028 requirements apply to software development initiatives;
(3) Security considerations for AI model development and use;
(4) The importance of the OWASP Top Ten project;
(5) How to leverage NIST SP 800-218 as a Secure Software Development Framework (SSDF); and
(6) A SCA Practitioner's obligations per the SCA's Code of Professional Conduct (CoPC).[14]

CONTINUING PROFESSIONAL EDUCATION (CPE) REQUIREMENTS
CSCAPs are expected to earn at least ten (10) hours of Continuing Professional Education (CPE) on an annual basis.

---

[7] *EO 14028 - https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity*
[8] *NIST SP 800-218 v1.1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf*
[9] *NIST SP 800-218A - https://csrc.nist.gov/pubs/sp/800/218/a/final*
[10] *NIST SP 800-160 Vol 1 Rev 1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf*
NIST SP 800-160 Vol 2 Rev 1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
[11] *OWASP Top 10 - https://owasp.org/www-project-top-ten/*
[12] *SCA BoK - https://content.securecodealliance.com/SCA-BoK.pdf*
[13] *SCA CoPC – https://securecodealliance.com/content/sca-copc.pdf*
[14] *SCA CoPC – https://securecodealliance.com/content/sca-copc.pdf*

Supporting Information

The following information addresses the administrative nature of the course:

Instructional Methods

The CSCAP training course is 100% Computer Based Training (CBP). This is an entirely Internet-based course. It is self-paced training and does not require face-to-face class meetings.

Course Communication and Feedback

The SAICO has no scheduled course communications, other than:

(1) Initial welcome/onboarding communications;
(2) Course completion certificate; and
(3) Student coursework feedback form.

The email address you provided to set up your training account will be the email used to send communications. To update your email address:

- In your profile, you can update the email address; or
- Contact SAICO support for assistance at support@securecontrolsframework.com.

Required Textbooks or Materials

There are no textbooks required. The material covered in this course is freely available online:

Technology Requirements

Students must have access to the Internet to participate in training. No special software is required other than a modern web browser. Student devices are expected to have a current operating system with updates installed and audio functionality (e.g., speakers, headphones, etc.) to listen to the educational videos (transcripts will be provided).

Minimum Student Technical Requirements/Skills

Minimum technical skills are needed in this course. All coursework must be completed and submitted online through the SAICO training portal. Therefore, students must have consistent and reliable access to a suitable computer and the Internet.

The minimum technical skills required include the ability to:

(1) Use of a personal device (e.g., Personal Computer (PC), tablet, smartphone, etc.) for Internet browsing, including use of audio functions;
(2) Organize and save electronic files;
(3) Use email and attached files;
(4) Download and upload documents; and
(5) Locate information with an Internet browser.

Technical Support

The SAICO does not provide technical support for student devices. Administrative support pertaining to the operation of the LMS is available through SAICO support at support@securecontrolsframework.com.

Assignments and Assessments

The SCA Practitioner training course is a Pass/Fail course. It is a self-paced curriculum that progresses from lesson to lesson. There are no assignments (e.g., project work, research papers, etc.) as part of the SCA Practitioner training course. However, there will be assessments:

(1) Quizzes at the end of each major section; and
(2) A final knowledge exam.

The SCA appreciates the nature of development operations, where software is rarely development in a vacuum. The global nature of software development also means that the English language is often not the native language for developers. Given this understanding of the global workforce and how collaboration efforts exist in software development, the practice of being able to openly reference content should be seen as an industry norm. Therefore, the CSCAP knowledge exam:

(1) Is open-book, where "open book" is defined as:
- **a. The following references are authorized:**
  - **i. SCA Body of Knowledge;**[15]
  - **ii. Executive Order (EO) 14028;**[16]
  - **iii. NIST SP 800-218 v1.1;** [17]
  - **iv. NIST SP 800-218A;**[18]
  - **v. NIST SP 800-160 (vol 1 & 2);** [19] **and**
  - **vi. OWASP Top Ten;** [20]
- **b. The following tools and/or resources are prohibited:**
  - **i. Artificial Intelligence (e.g., ChatGPT, Google Gemini, Microsoft Copilot, Claude, etc.); and**
  - **ii. Cheat sheets, including but not limited to:**
    1. **Condensed notes or information;**
    2. **Quick references; and**
    3. **Any other non-SCA approved study aid.**

(2) Has a maximum time limit of ninety (90) minutes;

(3) Consists of fifty (50):
- **a. True/False questions;**
- **b. Multiple-select questions; and**
- **c. Multiple-choice questions; and**

(4) Requires a minimum grade of seventy percent (70%) to pass. We selected this minimum grade because it:
- **a. Demonstrates a satisfactory understanding of the core concepts of the subject matter; and**
- **b. Maintains a higher standard for academic performance.**

The cost of the CSCAP training course includes one (1) attempt at taking the knowledge exam. Retaking the knowledge exam will incur an additional cost, unless the reason was due to a technical incident that precluded the student from completing the exam.

EQUAL OPPORTUNITY

The SAICO is committed to an environment that is inclusive, safe, and respectful for all persons. To achieve that, all course activities will be conducted in an atmosphere of friendly participation and interaction among colleagues, recognizing and appreciating the unique experiences, background, and point of view each student brings. Students are always expected to apply the highest academic standards to this course and to treat others with dignity and respect.

---

[15] *SCA BoK - https://content.securecodealliance.com/SCA-BoK.pdf*
[16] *EO 14028 - https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity*
[17] *NIST SP 800-218 v1.1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf*
[18] *NIST SP 800-218A - https://csrc.nist.gov/pubs/sp/800/218/a/final*
[19] *NIST SP 800-160 Vol 1 Rev 1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf*
NIST SP 800-160 Vol 2 Rev 1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
[20] *OWASP Top 10 - https://owasp.org/www-project-top-ten/*

GLOSSARY: ACRONYMS & DEFINITIONS

[Company Name] recognizes two sources for authoritative definitions:

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define common digital security terms;[21] and
- NIST Glossary.[22]

Security Requirements and Controls

The term control can be applied to a variety of contexts and can serve multiple purposes. When used in the security context, a security control can be a mechanism (e.g., a safeguard or countermeasure) designed to address protection needs that are specified by a set of security requirements.

- Controls are defined as the power to make decisions about how something is managed or how something is done; the ability to direct the actions of someone or something; an action, method or law that limits; or a device or mechanism used to regulate or guide the operation of a machine, apparatus or system.
- Requirements are defined as statements that translate or express a need and its associated constraints and conditions.[23]

[21] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*
[22] *NIST Glossary - https://csrc.nist.gov/glossary*
[23] *ISO/IEC/IEEE 29148*