SECURE CONTROLS FRAMEWORK ASSESSOR (SCF ASSESSOR) TRAINING

version 2025.2

PUBLIC

Public Release Authorized

Table of Contents

SCF Assessor & Instructor Certification Organization (SAICO) Overview

All SCF Assessor and Instructor Certification Organization (SAICO)-certified individuals are required to undergo foundational training.

The SAICO governs the training and certification of following roles within the SCF CAP Ecosystem:

(1) SCF Architect. SCF Architects are SAICO-certified individuals who have advanced SCF-related knowledge and competence necessary to:
   a. Architect and design SCF-based cybersecurity and data protection programs that are capable of addressing the tactical, operational and strategic needs of the organization specific to its unique People, Processes, Technologies, Data and Facilities (PPTDF) considerations.
   b. Assist SCF Practitioners with the implementation of SCF controls; and
   c. Make adjustments to the cybersecurity and data protection programs to account for new and/or changed laws, regulations and frameworks that affect the PPTDF.

(2) SCF Practitioner. SCF Practitioners are SAICO-certified individuals who have the knowledge and skills to:
   a. Implement SCF controls that align with the SCF recommended practices and structure; and
   b. Maintain an organization's cybersecurity and data protection program.

(3) SCF Assessor. SCF Assessors are SAICO-certified individuals who are:
   a. Qualified to participate in and/or lead a SCF Third-Party Assessment Organization's (3PAO's) assessment team to perform SCF Conformity Assessment Program (SCF CAP) assessments; and
   b. Knowledgeable to analyze SCF controls to determine if the control is appropriate, properly implemented and produces the desired results to meet Assessment Objectives (AOs).

(4) SCF Trainer. SCF Trainers are SAICO-certified individuals who are:
   a. Employed by a SCF Licensed Training Provider (SCF LTP); and
   b. Responsible for delivering initial and recurring SCF-based educational training for SAICO-approved individual-level certifications.

Note: SCF Licensed Training Providers (SCF LTPs) are SAICO-certified organizations that deliver a SAICO-approved individual-level certification training program using SCF Trainers.[1]

[1] *SCF Licensed Training Provider - https://securecontrolsframework.com/scf-licensed-training-providers/*

SCF Assessor Training Prerequisites

Knowledge Prerequisites

It is important to note that the SCF Assessor course is not designed to train students to think like an assessor/auditor, since that is a prerequisite skill that students are expected to already possess. The items listed below summarize the knowledge prerequisites necessary to be successful in the role of the SCF Assessor. Each topic listed below has a URL to the source document(s), so if you lack adequate proficiency in one, or more, topics, it is your responsibility to read the documentation to gain the requisite knowledge.

Have a proficient / conversational understanding of the following supplemental documentation:

- What Is the Secure Controls Framework (SCF) (e.g., structure, content, uses, etc.);[2]
- SCF Conformity Assessment Program (SCF CAP);[3]
- Cybersecurity & Data Protection Assessment Standards (CDPAS);[4]
- Integrated Controls Management (ICM) Model;[5]
- SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM);[6]
- SCF Cybersecurity & Data Privacy Risk Management Model (C|P-RMM);[7]
- Unified Scoping Guide (USG);[8]
- Cybersecurity risk tolerance & materiality concepts;[9]
- SCF CAP Code of Professional Conduct (CoPC);[10] and
- Proficient understanding of Set Theory Relationship Mapping (STRM).[11]

Education / Certification Prerequisites

The US Department of Defense Manual (DODM) 8140.03, Cybersecurity Workforce Qualification and Management Program, contains a listing of industry certifications for various cybersecurity-related positions.[12] Specific to the SCF CAP, the Security Control Assessor (role ID# 612) from DODM 8140.3 was designated as the industry standard to establish minimum certifications that are applicable to an SCF Assessor.

While there is only one certification for an SCF Assessor, there are specific requirements for the roles that an SCF Assessor can perform.

To serve as an **entry or intermediate-level assessor**, that individual must have at least one (1) of the following:

One (1) of the following certifications:

- **CGRC/CAP** - ISACA Certified in Governance, Risk, and Compliance (formerly known as CAP);
- **GSEC** - GIAC Security Essentials Certification;
- **CASP+** - CompTIA Advanced Security Practitioner plus;
- **Cloud+** - CompTIA Cloud plus;
- **PenTest+** - CompTIA Penetration Tester plus; and/or
- **Security+** - CompTIA Security plus.

OR

---

[2] *What is the SCF? https://securecontrolsframework.com/what-is-the-scf/*
[3] *SCF Conformity Assessment Program (SCF CAP) - https://securecontrolsframework.com/scf-conformity-assessment-program-cap/*
[4] *Cybersecurity & Data Protection Assessment Standards (CDPAS) - https://securecontrolsframework.com/cybersecurity-data-protection-assessment-standards-cdpas/*
[5] *Integrated Controls Management (ICM) model - https://securecontrolsframework.com/integrated-controls-management/*
[6] *SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) - https://securecontrolsframework.com/capability-maturity-model/*
[7] *SCF Cybersecurity & Data Privacy Risk Management Model (C|P-RMM) - https://securecontrolsframework.com/risk-management-model/*
[8] *Unified Scoping Guide (USG) - https://securecontrolsframework.com/content/cap/unified-scoping-guide-usg.pdf*
[9] *Cybersecurity risk tolerance & materiality - https://securecontrolsframework.com/cybersecurity-materiality/*
[10] *SCF CAP CoPC - https://securecontrolsframework.com/content/cap/scf-cap-copc.pdf*
[11] *NIST IR 8477-based STRM - https://securecontrolsframework.com/set-theory-relationship-mapping-strm/*
[12] *DoDM 8140.03 - https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf*

An undergraduate degree:

- From an:
  - Accreditation Board for Engineering and Technology (ABET) accredited; or
  - Centers of Academic Excellence (CAE) designated institution; and
- In the one of the following degrees (Bachelor of Science):
  - Information Technology (IT);
  - Cybersecurity;
  - Data Science;
  - Information Systems; or
  - Computer Science (CS).

For **senior-level SCF Assessors (or an SCF Assessor serving in the role of an Assessment Team Lead (ATL))**, that individual must have at least one (1) of the following:

One (1) of the following certifications:

- **CISM** - ISACA Certified Information Security Manager;
- **CISA** - ISACA Certified Information Systems Auditor;
- **CISSP** - ISC2 Certified Information Systems Security Professional;
- **CISSP-ISSEP** - ISC2 CISSP - Information Systems Security Engineering Professional;
- **GCSA** - GIAC Cloud Security Automation;
- **GSLC** - GIAC Security Leadership Certification;
- **GSNA** - GIAC Systems and Network Auditor;
- **CySA+** - CompTIA Cybersecurity Analyst plus;
- **C)ISSO** - Certified Information Systems Security Officer;
- **C)PTE** - Certified Penetration Testing Engineer; and/or
- **FIESP-A** - Federal IT Security Professional-Auditor.

OR

An undergraduate degree:

- From an:
  - Accreditation Board for Engineering and Technology (ABET) accredited; or
  - Centers of Academic Excellence (CAE) designated institution; and
- In the one of the following degrees (Bachelor of Science):
  - Information Technology (IT);
  - Cybersecurity;
  - Data Science;
  - Information Systems; or
  - Computer Science (CS).

Secure Controls Framework Assessor (SCF Assessor) Training Overview

Course Title
Secure Controls Framework Assessor (SCF Assessor) Training

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

Course Cost & Certification Lifecycle
SAICO certifications are valid for a duration of one (1) year from issuance, at which point the certificate must be renewed or it is expired. The renewal process includes paying an annual certification maintenance fee and taking a knowledge test to ensure the individual's proficiency in the subject matter.

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

Description	Course Fee (one time)	Certification Maintenance (annual)
SCF Assessor Training	$500	$250
Knowledge Exam License (retakes)	$100	N/A

Course Registration
Prospective students can sign up for SCF Assessor training online at: https://training.securecontrolsframework.com

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 six (6) hours to complete the SCF Assessor training. If students are unfamiliar with the supporting documentation, they should plan to allocate additional study time to become familiar with the material because this course utilizes them as prerequisites.

Course Description
SCF Assessor training prepares students to participate in a SCF Third-Party Assessment Organization's (3PAO) assessment team to conduct SCF-related Third-Party Assessment, Attestation and Certification Services (3PAAC Services). The SCF Assessor course is not designed to train students to think like an assessor/auditor, since that is a prerequisite skill.

The SCF Assessor training course is designed to refine a student's existing knowledge of the following core concepts:
(1) The structure and content of:
    a. Secure Controls Framework (SCF); and
    b. SCF Conformity Assessment Program (SCF CAP);
(2) The assessment standards used to perform SCF-related 3PAAC Services;
(3) Scoping the assessment using the Unified Scoping Guide (USG);
(4) Cybersecurity risk tolerance & materiality concepts; and
(5) The SCF CAP Code of Professional Conduct (CoPC).

Successfully completing training and passing the knowledge exam will provide the student with the designation as a SCF Assessor.

COURSE LEARNING OUTCOMES

After successful completion of this course and earning the SCF Assessor designation, students will be able to converse with clients and other members of the SCF Ecosystem about the following topics. SCF Assessors will be expected to be able to:

(1) Discuss the structure and content of:
   a. Secure Controls Framework (SCF);
   b. Assessment Objectives (AOs);
   c. Evidence Request List (ERL); and
   d. SCF Conformity Assessment Program Body of Knowledge (SCF CAP BoK).

(2) Describe the various members of the SCF CAP Ecosystem, including pertinent roles and responsibilities.

(3) Demonstrate the application of the Cybersecurity & Data Protection Assessment Standards (CDPAS) as the underlying standard used in the SCF CAP.

(4) Describe how the following frameworks may be used in a SCF assessment:
   a. NIST IR 8477-based Set Theory Relationship Mapping (STRM);
   b. Unified Scoping Guide (USG);
   c. Integrated Controls Management (ICM) model;
   d. SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM); and
   e. SCF Cybersecurity & Data Privacy Risk Management Model (C|P-RMM).

(5) Describe the roles and requirements assigned to:
   a. Organization Seeking Assessment (OSA);
   b. Assessors; and
   c. 3PAOs.

(6) Describe the following concepts, as it relates to SCF CAP assessments:
   a. Cybersecurity risk tolerance & materiality concepts;
   b. What constitutes passing / failing a SCF CAP assessment, per the SCF CAP BoK;
   c. An SCF Assessor's obligations per the SCF CAP Code of Professional Conduct (CoPC).

(7) Leverage the SCF Connect tool to:
   a. Initiate an SCF CAP assessment;
   b. Provision OSA user accounts;
   c. Collect required assessment evidence using the SCF ERL;
   d. Conduct a SCF CAP assessment;
   e. Assess evidence of control implementation; and
   f. Generate SCF CAP Report on Conformity (RoC) assessment reports.

CONTINUING PROFESSIONAL EDUCATION (CPE) REQUIREMENTS

Annually, SCF Assessors are expected to complete at least twenty (20) hours of Continuing Professional Education (CPE) training in topics relevant to the skills and situational awareness necessary to be an effective SCF Assessor.

SUPPORTING INFORMATION

The following information addresses the administrative nature of the course:

INSTRUCTIONAL METHODS

The SCF Assessor 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.
- Additional training is available through certified SCF Trainers.

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:

(1) What the Secure Controls Framework (SCF) (e.g., structure, content, uses, etc.);[13]
(2) Integrated Controls Management (ICM) Model;[14]
(3) SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM);[15]
(4) SCF Cybersecurity & Data Privacy Risk Management Model (C|P-RMM);[16]
(5) Cybersecurity risk tolerance & materiality concepts;[17]
(6) Unified Scoping Guide (USG);[18]
(7) Proficient understanding of Set Theory Relationship Mapping (STRM);[19]
(8) SCF CAP Code of Professional Conduct (CoPC);[20]
(9) SCF Conformity Assessment Program (SCF CAP);[21]
(10) SCF CAP Code of Professional Conduct (CoPC);[22] and
(11) Cybersecurity & Data Protection Assessment Standards (CDPAS).[23]

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).

---

[13] *What is the SCF? https://securecontrolsframework.com/what-is-the-scf/*
[14] *Integrated Controls Management (ICM) model - https://securecontrolsframework.com/integrated-controls-management/*
[15] *SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) - https://securecontrolsframework.com/capability-maturity-model/*
[16] *SCF Cybersecurity & Data Privacy Risk Management Model (C|P-RMM) - https://securecontrolsframework.com/risk-management-model/*
[17] *Cybersecurity risk tolerance & materiality - https://securecontrolsframework.com/cybersecurity-materiality/*
[18] *Unified Scoping Guide (USG) - https://securecontrolsframework.com/content/cap/unified-scoping-guide-usg.pdf*
[19] *NIST IR 8477-based STRM - https://securecontrolsframework.com/set-theory-relationship-mapping-strm/*
[20] *SCF CAP Code of Professional Conduct (CoPC) - https://securecontrolsframework.com/content/cap/scf-cap-copc.pdf*
[21] *SCF Conformity Assessment Program (SCF CAP) - https://securecontrolsframework.com/scf-conformity-assessment-program-cap/*
[22] *SCF CAP CoPC - https://securecontrolsframework.com/content/cap/scf-cap-copc.pdf*
[23] *Cybersecurity & Data Protection Assessment Standards (CDPAS) - https://securecontrolsframework.com/cybersecurity-data-protection-assessment-standards-cdpas/*

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 SCF Assessor 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 SCF Assessor training course. However, there will be assessments:

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

The knowledge exam:

(1) Is a closed-book exam;
(2) Has a maximum time limit of two (2) hours; and
(3) Consists of one hundred (100):
    a. True/False questions;
    b. Multiple-select questions; and
    c. Multiple-choice questions.
(4) Requires a minimum grade of seventy-five percent (75%) 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 SCF Assessor 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.

Academic Integrity

Students are expected to practice the highest possible standards of academic integrity. Any deviation from this expectation will result in:

(1) A failing grade on the SCF Assessor training course; and
(2) Review for future eligibility for participation in the SCF CAP ecosystem, due to a violation of a SCF CAP Code of Professional Conduct (CoPC) principes.

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.

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;[24] and
- NIST Glossary.[25]

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.[26]

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