SECURE CONTROLS FRAMEWORK SCF ARCHITECT (SCF ARCHITECT) 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/*

Understanding The Difference Between The SCF Practitioner and SCF Architect Roles

Strategic Program Architecture & Design

While SCF Practitioners focus on implementing specific controls within established frameworks, SCF Architects design the entire program architecture that enables those implementations. SCF Architects are expected to:

(1) Develop enterprise-wide governance structures, create strategic roadmaps spanning multiple years and establish the architectural foundations that connect security initiatives to business strategy.

(2) Must understand how to integrate SCF across diverse organizational structures, design scalable frameworks adaptable to evolving requirements and create the systematic approach that SCF Practitioners will follow when implementing controls.

In this context, an SCF Architect is expected to have familiarity with:

- Business alignment through Cybersecurity & Data Privacy by Design (C|P) principles.
- Long-term security roadmap development using Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM).
- Enterprise-wide security program design methodologies.
- Integration of SCF into organizational governance structures.
- Security architecture frameworks and alignment with SCF.
- Designing scalable security programs across complex organizations.

Program Leadership & Governance Design

SCF Practitioners operate within established governance structures and reporting relationships, while SCF Architects design the governance frameworks themselves and leadership approaches that drive program success. SCF Architects are expected to:

(1) Develop committee structures, create stakeholder engagement models, design executive reporting approaches and establish metrics frameworks for program oversight.

(2) Understand how to build the leadership structures necessary for effective security program management, including decision rights, escalation paths and communication strategies.

In this context, an SCF Architect is expected to have familiarity with:

- Security governance committee structures.
- Roles and responsibilities design (e.g., NIST NICE Cybersecurity Workforce Framework).
- Cross-functional collaboration models.
- Executive reporting frameworks.
- Metrics dashboard design.
- Communication strategies.
- Budget and resource allocation models.

Advanced SCF Implementation

SCF Practitioners implement SCF controls according to established guidance, while SCF Architects customize and extend the framework to address unique organizational requirements. SCF Architects are expected to:

(1) Develop methodologies for framework tailoring, create organization-specific control statements, design integration approaches with other frameworks and establish governance for framework customization.

(2) Understand how to maintain framework integrity while adapting SCF to fit specific statutory, regulatory, industrial and organizational contexts.

In this context, an SCF Architect is expected to have familiarity with:

- SCF Conformity Assessment Program (SCF CAP) conformity assessment preparation.
- SCF customization for industry-specific requirements.
- SCF extension methodologies for unique environments.
- SCF-based policy architecture development.
- Framework integration with existing governance structures.
- Custom control development methodologies.
- Control mapping and cross-framework alignment.

Advanced Risk Management

Practitioners typically identify and address specific risks through control implementation, while SCF Architects design the entire risk management framework that guides those activities. SCF Architects are expected to:

(1) Develop quantitative risk methodologies, create enterprise risk models, establish risk governance structures and design the processes for consistent risk evaluation.

(2) Understand how to translate technical risks into business impacts, develop risk appetites aligned with organizational objectives and create the comprehensive risk frameworks that SCF Practitioners use to assess individual risks.

In this context, an SCF Architect is expected to have familiarity with:

- Enterprise risk modeling techniques using Cybersecurity & Data Privacy Risk Management Model (C|P-RMM).
- Risk appetite framework development using SCF cybersecurity materiality concepts.
- Quantitative and qualitative risk analysis methodologies.
- Threat catalog development and management.
- Risk governance structures and processes.
- Material control identification and prioritization.
- Cross-domain risk assessment strategies.

Compliance Landscape

SCF Practitioners focus on implementing controls to meet specific compliance requirements, while SCF Architects design unified compliance architectures that efficiently address multiple regulatory frameworks. SCF Architects are expected to:

(1) Develop cross-mapping methodologies, create consolidated control sets, design optimized assessment approaches and establish governance for maintaining compliance as regulations evolve.

(2) Understand the complex relationships between different frameworks and how to create efficient structures that reduce duplication and inconsistency while ensuring comprehensive coverage.

In this context, an SCF Architect is expected to have familiarity with:

- Using the Integrated Controls Management (ICM) to address complex compliance requirements.
- Multi-framework harmonization with SCF as foundation.
- Cross-regulatory compliance architecture.
- Jurisdictional variations in compliance requirements.
- Future-proofing compliance programs.
- Reciprocity strategies between overlapping compliance frameworks.
- Evidence collection and validation methodologies based on Cybersecurity & Data Protection Assessment Standards (CDPAS).

Building Towards Maturity

SCF Practitioners operate within established maturity levels, implementing controls to meet defined targets, while SCF Architects, design the maturity models themselves, establishing capability levels, progression metrics and transformation roadmaps. SCF Architects are expected to:

(1) Create assessment methodologies, define target states aligned with business objectives and develop strategies for capability enhancement.

(2) Understand how to evaluate current capabilities, establish realistic maturity targets and create the programmatic approach to systematically advancing security maturity across the organization.

In this context, an SCF Architect is expected to have familiarity with:

- Maturity model implementation using C|P-CMM.
- Program capability advancement strategies across C|P-CMM maturity levels L0-L5.
- Metrics design for demonstrating program evolution.
- Benchmark development against industry standards.
- Continuous improvement architecture.
- Maturity assessment methodologies.
- Transition planning between maturity levels.

Complex Integration

SCF Practitioners implement specific security and privacy controls, often within separate domains, while SCF Architects design unified protection frameworks that integrate security and privacy requirements into cohesive architectures. SCF Architects are expected to:

(1) Develop data governance structures, create privacy-by-design methodologies, establish data classification schemas and design the integrated policies that ensure consistent protection.
(2) Understand the complex relationships between security and privacy requirements and how to create architectures that address both domains efficiently and effectively.

In this context, an SCF Architect is expected to have familiarity with:

- Data-centric security architecture principles.
- Privacy engineering fundamentals through SCF Data Privacy Management Principles.
- Privacy by design implementation strategies.
- Data protection architectural patterns.
- Cross-functional security and privacy controls integration.
- Data classification and handling architectures.
- Privacy impact assessment methodologies.

Third-Party Risk SCF Architectural Frameworks

SCF Practitioners typically execute third-party / vendor assessments according to established methodologies, while SCF Architects design the assessment frameworks themselves and integration with enterprise risk processes. SCF Architects are expected to:

(1) Develop supply chain security architectures, create contractual security requirement templates, design tiered assessment methodologies and establish governance for managing third-party risk.
(2) Understand how to build comprehensive programs that address risks across the entire supply chain while optimizing assessment resources and ensuring consistent evaluation.

In this context, an SCF Architect is expected to have familiarity with:

- Supply chain security architecture.
- Vendor assessment integration strategies.
- Third-party governance program design.
- Contractual security requirements framework development.
- Vendor risk quantification models.
- Third-party attestation evaluation methodologies.
- Supply chain risk management program design.

Security Technology SCF Architecture

SCF Practitioners implement and operate security technologies according to defined standards, while SCF Architects design the security technology ecosystem itself and how it aligns with control requirements. SCF Architects are expected to:

(1) Develop reference architectures, create technology roadmaps, design security patterns and establish governance for technology decisions.
(2) Understand how to build cohesive technology environments that efficiently implement controls rather than collections of point solutions, including capability mapping, integration strategies and optimization approaches.

In this context, an SCF Architect is expected to have familiarity with:

- Security technology stack design principles.
- Security capabilities mapping to control requirements.
- Technology rationalization methodologies.
- Security architecture review processes.
- Security technology roadmap development.
- Control technology integration patterns.
- Security automation architectures.

Secure Controls Framework SCF Architect (SCF Architect) Training Overview

Course Title
Secure Controls Framework SCF Architect (SCF Architect) Training

Online Course Access
Students have one hundred eighty (180) days from the date of purchase to complete SCF Architect 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 Architect Training	$250	$250*
Knowledge Exam License (retakes)	$100	N/A

* *NOTE - Upon obtaining status as a SCF Architect, there is no need to perform annual renewals of the SCF Practitioner certification, just the SCF Architect certification.*

Course Registration
Prospective students can sign up for SCF Architect 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 Architect 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 Architects are SAICO-certified individuals who have the knowledge and skills to 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. The SCF Architect course is not designed to train students to think like an architect, since that is a prerequisite skill.

The SCF Architect 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 Architect.

PREREQUISITES:
Students are required to meet minimum education and certification requirements to be a SCF Architect:

(1) Current SCF Practitioner certification;*
(2) Minimum of five (5) years' experience as full-time cybersecurity professional; and
(3) Familiarity with the following publications / resources:
    a. What Is the Secure Controls Framework (SCF) (e.g., structure, content, uses, etc.);[2]
    b. Integrated Controls Management (ICM) Model;[3]
    c. SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM);[4]
    d. SCF Cybersecurity & Data Privacy Risk Management Model (C|P-RMM);[5]
    e. Unified Scoping Guide (USG);[6]
    f. Cybersecurity risk tolerance & materiality concepts;[7]
    g. NIST IR 8477 - Set Theory Relationship Mapping (STRM);[8]
    h. SCF Conformity Assessment Program (SCF CAP);[9]
    i. SCF CAP Code of Professional Conduct (CoPC);[10] and
    j. Cybersecurity & Data Protection Assessment Standards (CDPAS);[11]

* *NOTE - Upon obtaining status as a SCF Architect, there is no need to perform annual renewals of the SCF Practitioner certification, just the SCF Architect certification.*

COURSE LEARNING OUTCOMES
After successful completion of this course and earning the SCF Architect designation, students will be able to converse with clients and other members of the SCF Ecosystem about the following topics. SCF Architects 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 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:

---

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

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 Architect'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

The SCF Practitioner role does not require a minimum number of Continuing Professional Education (CPE) requirements that must be completed on an annual basis.

Supporting Information

The following information addresses the administrative nature of the course:

Instructional Methods

The SCF Practitioner 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.);[12]
(2) Integrated Controls Management (ICM) Model;[13]
(3) SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM);[14]
(4) SCF Cybersecurity & Data Privacy Risk Management Model (C|P-RMM);[15]
(5) Cybersecurity risk tolerance & materiality concepts;[16]
(6) Unified Scoping Guide (USG);[17]
(7) Proficient understanding of Set Theory Relationship Mapping (STRM);[18]
(8) SCF CAP Code of Professional Conduct (CoPC);[19]
(9) SCF Conformity Assessment Program (SCF CAP);[20]
(10) SCF CAP Code of Professional Conduct (CoPC);[21] and
(11) Cybersecurity & Data Protection Assessment Standards (CDPAS).[22]

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).

---

[12] *What is the SCF? https://securecontrolsframework.com/what-is-the-scf/*
[13] *Integrated Controls Management (ICM) model - https://securecontrolsframework.com/integrated-controls-management/*
[14] *SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) - https://securecontrolsframework.com/capability-maturity-model/*
[15] *SCF Cybersecurity & Data Privacy Risk Management Model (C|P-RMM) - https://securecontrolsframework.com/risk-management-model/*
[16] *Cybersecurity risk tolerance & materiality - https://securecontrolsframework.com/cybersecurity-materiality/*
[17] *Unified Scoping Guide (USG) - https://securecontrolsframework.com/content/cap/unified-scoping-guide-usg.pdf*
[18] *NIST IR 8477-based STRM - https://securecontrolsframework.com/set-theory-relationship-mapping-strm/*
[19] *SCF CAP Code of Professional Conduct (CoPC) - https://securecontrolsframework.com/content/cap/scf-cap-copc.pdf*
[20] *SCF Conformity Assessment Program (SCF CAP) - https://securecontrolsframework.com/scf-conformity-assessment-program-cap/*
[21] *SCF CAP CoPC - https://securecontrolsframework.com/content/cap/scf-cap-copc.pdf*
[22] *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 Architect 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 Architect 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 eighty percent (80%) 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 Architect 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 Architect 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;[23] and
- NIST Glossary.[24]

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.[25]

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