SECURE CONTROLS FRAMEWORK CONFORMITY ASSESSMENT PROGRAM (SCF CAP)

CODE OF PROFESSIONAL CONDUCT

Version 2025.1

This publication is available free of charge from: **https://securecontrolsframework.com/content/cap/scf-cap-copc.pdf**

Table of Contents

FOREWORD

The mission of the Secure Controls Framework (SCF) is to provide a powerful tool and methodology that will advance how cybersecurity and data protection controls are implemented and assessed at an organization's strategic, operational and tactical layers, regardless of its size or industry.

The Secure Control Framework Council (SCF Council) established the SCF Conformity Assessment Program (SCF CAP) as a structure to conduct cybersecurity and data protection-related Third-Party Assessment, Attestation and Certification Services (3PAAC Services). There is a need for a scalable and cost-effective solution to obtain a company-level, third-party assessment of cybersecurity & data protection practices and the SCF CAP addresses that need.

The SCF CAP Ecosystem parties have an influential and privileged position within the SCF CAP, and these parties must be able to account for the decisions made and the behaviors displayed.

PURPOSE

The purpose of the SCF CAP Code of Professional Conduct (CoPC) is fourfold:

1. Establish clear, precise, ethical and professional guidelines;
2. Ensure accountability within the SCF CAP Ecosystem;
3. Provide minimum standards by which to judge conduct; and
4. Encourage a culture of integrity, collaboration, and trust among ecosystem participants.

The CoPC establishes the ethical and professional standards required for participants operating within the SCF CAP Ecosystem, as well as the procedures for investigating and adjudicating violations of the CoPC. It also provides guidance for SCF CAP Ecosystem participants on navigating prospective conflicts-of-interest and other impartiality issues that might arise while conducting SCF CAP-related activities.

INTENT

The intent of the CoPC is for individuals, entities and groups operating within the SCF CAP Ecosystem to:

1. Uphold and enhance the credibility and reputation of the SCF CAP through ethical and professional behavior;
2. Adhere to SCF CAP Third-Party Assessment, Attestation & Certification (3PAAC) standards;
3. Be honest, impartial and committed to conducting rigorous, objective and fair assessments;
4. Adhere to professional conduct with truth, accuracy, fairness, responsibility and objectivity;
5. Avoid Conflicts of Interest (COI), including perceived COI;
6. Act professionally and objectively under adverse pressure by seeking clarification from The Cyber AB for matters that are unclear or need authoritative guidance;
7. Honestly represent professional qualifications, competence and/or experience;
8. Treat all information gained in relation to SCF CAP 3PAAC Services in a confidential and sensitive manner;
9. Preface any public statements by clearly indicating on whose behalf the statement(s) are made;
10. Ensure peer opinions are respected and professional conduct governed to ensure that honesty and openness is demonstrated within a 3PAO's assessment team;
11. React openly and professionally in the event of non-ethical behavior; and
12. Protect material concerning SCF CAP assessments from unauthorized disclosure.

SCOPE

This CoPC represents the professional performance standards to which the members of the SCF CAP Ecosystem will be held accountable and the procedures for addressing violations of those standards.

CoPC applies to all individuals, entities and groups operating within the SCF CAP Ecosystem, to include:

- The Cyber AB, including its professional staff and Board of Directors;
- The SCF Assessor and Instructor Certification Organization (SAICO), including its professional staff;

- SCF Council members, advisory board and contributors;
- SCF Third-Party Assessment Organizations (SCF 3PAOs);
- SCF Registered Provider Organizations (SCF RPOs);
- SCF Authorized Platform Organizations (SCF APOs);
- SCF Licensed Content Providers (SCF LCPs);
- SCF Approved Training Providers (SCF ATPs);
- SCF Practitioners; and
- SCF Assessors.

Organizations Seeking Assessment (OSAs) and SCF Certified Organizations are not bound to the CoPC but are encouraged to adopt its practices, wherever applicable.

CoPC Violation Incidents (CoPC VI)

Violations of the SCF CAP Ecosystem Code of Conduct are taken very seriously by The Cyber AB and SCF Council.

The Cyber AB will:

1. Maintain a capability to intake reports from the SCF Community on a possible CoPC Violation Incidents (CoPC VI).
2. Review all reports of CoPC VI for legitimacy.
3. Maintain a register of reported instances of CoPC VI.
4. Notify the SCF CAP Ecosystem party(ies) of the reported CoPC VI.
5. Implement appropriate disciplinary action(s) for actual instances of a CoPC VI.

Disciplinary action for CoPC VI includes:

1. Issuing a formal warning letter with steps to remediation and/or avoid future CoPC VI.
2. Revoking (in part or in full) the status of the offending SCF CAP Ecosystem party(ies).
3. Implementing a permanent ban from rejoining the SCF CAP Ecosystem.

Liability Limitations

THIS CONTENT IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE CONTENT OR THE USE OR OTHER DEALINGS IN THE CONTENT.

Submit comments on this publication to: cap@securecontrolsframework.com

SCF CAP Guiding Principles

The CoPC is based on a set of guiding principles. A violation of one (1) or more guiding principle(s) is considered CoPC Violation Incidents (CoPC VI). The eight (8) CoPC guiding principles are:

1. Professionalism: conducting activities with honesty, fairness and respect for others;
2. Impartiality: avoiding COI and maintaining unbiased decision-making;
3. Confidentiality: protecting sensitive data and proprietary information;
4. Information Integrity: ensuring the accuracy and security of information;
5. Lawful and Ethical Behavior: complying with all applicable laws and regulations;
6. Equal Opportunity: promoting inclusivity and refraining from discriminatory behavior;
7. Due Diligence & Due Care: employing practices to demonstrate due diligence and due care; and
8. Acceptable Use of Technologies: using technologies in secure and compliant ways.

The CoPC practices are derived from these fundamental principles and are to be regarded as mandatory professional standards. All participants within the SCF CAP Ecosystem are expected to uphold these principles and practices in all activities that relate to carrying out their roles within the SCF CAP.

Principle 1 - Professionalism

Within the SCF CAP, Professionalism includes the following practices:

1. Representing oneself and one's organization accurately and completely. This includes prohibiting:
    a. Misrepresenting any professional credentials or status; nor
    b. Exaggerating the services that you, or your company, are capable of and/or authorized to, deliver;
2. Being honest and factual in all dealings with colleagues, clients, trainees and others with whom you interact in your role as a member of the SCF CAP Ecosystem;
3. Conducting activities that do not negatively impact the prestige of the:
    a. SCF CAP Ecosystem;
    b. The Cyber AB;
    c. SCF Council; and/or
    d. SAICO;
4. Communicating truthful, not false or misleading information;
5. Refraining from accepting gifts or hospitality from SCF CAP Ecosystem members, for any reason or purpose;
6. Fulfilling all commitments as established by applicable SCF CAP contractual, license, certification or registration agreements;
7. Charging a fair and reasonable price for services rendered, to include refraining from:
    a. Offering a deceptively or unrealistically low price ("low-balling"); or
    b. Charging a price that is grossly in excess of reasonable costs during unique circumstances ("price gouging");
8. Foregoing guarantees of assessment or certification results, including:
    a. Guarantees that an OSA will succeed in its SCF CAP assessment if it engages with a credentialed individual or authorized organization; and/or
    b. Offering a "money back" guarantee or guaranteeing that individuals will pass a certification examination by taking a specific training program;
9. Refraining from making false or damaging statements about another member of the SCF CAP Ecosystem through online platforms, media outlets or other public communications with the intent to:
    a. Harm another party's reputation; or
    b. Grossly and/or recklessly disparaging another party; and
10. Maintaining transparency when explaining decisions, ensuring affected parties understand the rationale behind impartial determinations; and
11. Foregoing making premature assertions or declarations about outcomes of assessments or other results-based SCF CAP activities.

Principle 2 - Impartiality

When an individual or an organization engages in the SCF CAP, there must be absolute confidence that all parties will be treated fairly, impartially, without bias and that others in the SCF CAP Ecosystem will not receive any inappropriate preferences or acts of favoritism. Impartiality is the core of what instills trust and confidence in the SCF CAP. Therefore, the SCF CAP Ecosystem must operate free of any undue commercial, personal, financial or other pressures that could compromise the impartiality of SCF CAP assessments and certifications.

Within the SCF CAP, Impartiality includes the following practices:

1. Disclosing and mitigating Conflicts of Interest (COI) in a proactive and timely manner, including documenting the conflict and informing all affected parties of a SCF CAP activity. For any instances of COI that would compromise the impartiality of an impending or ongoing SCF CAP conformity assessment, SCF CAP Ecosystem members shall disclose to The Cyber AB, as soon as it is known, or reasonably should be known.
2. Complying with COI prohibitions as expressed in the CoPC and its appendices;
3. Avoiding participation in any activity, practice or transaction that could result in an actual or perceived COI;
4. Prohibiting SCF CAP Ecosystem members from participating in the SCF CAP conformity assessment process for an assessment in which they have a COI;
5. Ensuring all OSAs are subject to the same standards of assessment, regardless of the OSA's size, influence or reputation;
6. Basing evaluative decisions on factual evidence and standardized processes while avoiding personal opinions and/or biases that could influence outcomes;
7. Refraining from soliciting business or engaging in discussions about future consulting engagements with clients during active certification assessments;
8. Maintaining clear boundaries between roles (e.g., assessor, instructor, practitioner) to ensure no COI or undue influence arise from overlapping responsibilities; and
9. Mitigating or avoiding the appearance of perceived COI.

For more information on COI and how they can undermine impartiality, please see the Conflicts of Interest section of the CoPC.

Principle 3 - Confidentiality

All SCF CAP Ecosystem members should respect, protect and maintain the confidentiality of other parties' data. In carrying out SCF CAP activities, SCF CAP Ecosystem members may be made aware of certain confidential information that is acquired in the performance of professional services. This information might include, but is not necessarily limited to, proprietary data, trade secrets, business strategies, security postures and personal information that may be contained within various information systems. SCF CAP Ecosystem members must treat confidential information with the utmost care and under no circumstances reveal information learned during the delivery of SCF CAP services to anyone who is not expressly authorized to view it.

Within the SCF CAP, Confidentiality includes the following practices:

1. Maintaining the confidentiality of OSA data to preclude unauthorized disclosure;
2. Exercising due care to ensure that confidential, or privileged, information gathered during SCF CAP assessments, or consulting engagements, remains so, even after the work has ended; and
3. Refraining from copying or storing proprietary information, or materials, from external entities without explicit permission to do so.

Principle 4 - Information Integrity

The integrity of the SCF CAP Ecosystem is only as good as the integrity of the information that underpins all SCF CAP activities. SCF CAP assessment information, provided by OSAs and collected and reported by the 3PAOs, must be authentic and accurate.

Within the SCF CAP, Information Integrity includes the following practices:

1. Ensuring the accuracy, authenticity and security of all information discovered, or received, during the course of delivering SCF CAP services;
2. Reporting results and data from SCF CAP conformity assessments objectively, completely, clearly and accurately; and
3. Utilizing official training content developed by a SCF CAP training organization approved by the SAICO in all SCF CAP certification courses.

PRINCIPLE 5 - LAWFUL AND ETHICAL BEHAVIOR

The success of SCF CAP is reliant upon the lawful, ethical and respectful behavior of all SCF CAP Ecosystem members. Individuals and organizations participating in the SCF CAP should be able to rely upon the presumption that their peers, customers, competitors and overseers are operating lawfully and in mutual good faith.

Within the SCF CAP, Legal and Ethical Behavior includes the following practices:

1. Having and maintaining a satisfactory record of integrity and business ethics;
2. Telling the truth in all interactions within the SCF CAP Ecosystem and with The Cyber AB, the SCF Council and the SAICO;
3. Refraining from:
    a. Obtaining, attempting to obtain and/or assisting others in obtaining or maintaining a Cyber AB, SCF Council or SAICO:
        i. Unauthorized use of The Cyber AB, SCF Council or SAICO:
            1. Credentials;
            2. Badges; and/or
            3. Other symbols and marks; and/or
        ii. Misrepresenting the status of:
            1. Authorization;
            2. Accreditation;
            3. Certification;
            4. Designation;
            5. Registration;
            6. Approval; and/or
            7. Other affiliation;
4. Prohibiting any forms of harassment and/or discrimination in all interactions with individuals whom one encounters in connection with a role in the SCF CAP Ecosystem;
5. Obeying pertinent statutory, regulatory and contractual obligations that are applicable based on federal, state, local, tribal, territorial and international jurisdictions including refraining from:
    a. Committing any crime of:
        i. Intellectual Property (IP) infringement:
            1. Copyright infringement including:
                a. Using copyright protected logos without permission;
                b. Downloading copyright protected content without paying for it or getting permission;
                c. Using copyright protected images without permission;
                d. Copying copyright protected images or literary works, without a license or written agreement;
                e. Creating derivative works of copyright protected content without permission;
                f. Manufacturing and selling merchandise with copyright protected words or images;
            2. Trademark infringement including the unauthorized use of a:
                a. Trademark; and/or
                b. Service mark;
        ii. Fraud;
        iii. Bribery;
        iv. Larceny;
        v. Embezzlement;
        vi. Misappropriation of funds;

vii. Misrepresentation;
viii. Perjury; and/or
ix. Making false statements to law enforcement officials; and/or

b. Conspiracy to conceal or a similar offense in any legal proceeding, civil or criminal, whether or not in connection with activities that relate to carrying out a role in the SCF CAP Ecosystem;

6. Reporting to The Cyber AB within thirty (30) days of any:
   a. Indictments;
   b. Convictions;
   c. Guilty pleas or no-contest pleas to:
      i. Crimes of fraud;
      ii. Bribery;
      iii. Larceny;
      iv. Embezzlement;
      v. Misappropriation of funds;
      vi. Misrepresentation;
      vii. Perjury; and/or
      viii. Making false statements to law enforcement officials; and/or
   d. Conspiracy to conceal, or a similar offense, in any legal proceeding, civil or criminal, whether in connection with activities that relate to carrying out a role in the SCF CAP ecosystem; and/or
7. Refraining from and prohibiting:
   a. Cheating, assisting another in cheating, and/or allowing cheating on SCF CAP examinations.

   b. Cheating includes unauthorized, reproducing, distributing, displaying, discussing, sharing and/or otherwise misusing test questions and/or any part of test questions before, during or after an examination.

PRINCIPLE 6 - EQUAL OPPORTUNITY

The SCF CAP Ecosystem is open and welcoming to all. The Cyber AB is committed to ensuring that equal opportunity exists for all SCF CAP stakeholders and that the SCF CAP Ecosystem is free from discrimination and bias.

- Every individual and organization shall be treated fairly and equally within the SCF CAP; and
- All will have equal access to the professional, financial, authorization, accreditation and certification opportunities that the SCF CAP may afford.

Within the SCF CAP, Equal Opportunity includes the following practices:

1. In all interactions with individuals and organizations whom one encounters in connection with engaged in SCF CAP activities, prohibiting discrimination based on:
   a. Race;
   b. Skin color;
   c. Religion;
   d. Ancestry or national origin;
   e. Sex;
   f. Age;
   g. Marital status;
   h. Sexual orientation;
   i. Gender identity;
   j. Disability; and/or
   k. Political affiliation;
2. Respecting cultural differences within the SCF CAP Ecosystem; and
3. Being respectful to others in all SCF CAP-related conduct and speech.

Principle 7 – Due Diligence & Due Care

The performance of due diligence and due care practices are paramount to the attainment of consistency in SCF CAP Ecosystem. While some measure of discretion is granted to the judgement and experience of SCF CAP Assessors and SCF CAP Instructors, the backbone of SCF CAP consistency is the unwavering reliance upon and employment of officially approved processes, procedures, methodologies and curricula.

Within the SCF CAP, Due Diligence and Due Care includes the following practices:

1. Relying upon and adhering to, the authoritative:
    a. SCF CAP Body of Knowledge (SCF CAP BoK);[1] and/or
    b. Framework-specific SCF CAP conformity assessment Guide (AG); and
2. Teaching SCF CAP certification courses only with approved SCF CAP training content developed by, or authorized by, the SAICO.

Principle 8 - Acceptable Use of Technologies

All SCF CAP Ecosystem members must ensure the responsible and ethical use of technology-related systems, applications and services, including Artificial Intelligence and Autonomous Technologies (AAT), in their conduct of SCF CAP activities.

Within the SCF CAP, Acceptable Use of Technologies includes the following practices:

1. Ensuring transparency in technology employment in SCF CAP activities;
2. Upholding data privacy and security when employing technology solutions;
3. Prohibit reliance on AAT systems without human oversight during critical assessments;
4. Avoiding use of AAT that renders subservient or diminishes the authority and autonomy of SCF CAP Assessors in a SCF CAP certification assessment;
5. Avoiding biases in AAT used for assessment preparation and assessment conduct; and
6. Prohibiting providing customer data to an Internet-accessible AAT.

[1] *SCF CAP BoK - https://securecontrolsframework.com/content/cap/scf-cap-bok.pdf*

ACTUAL & PERCEIVED CONFLICTS OF INTEREST (COI)

The Cyber AB, SCF Council and SAICO are precluded from providing advice or issuing a "COI opinion" to a 3PAO or any member of an SCF CAP conformity assessment team. However, examples of hypothetical COI scenarios and their prospective resolution are provided for reference in Appendix A.

COI, both organizational and individual, could be based on financial, business, familial or other relationships, such as:

1. Financial interest in the OSA;
2. Business partnership or teaming relationship with the OSA;
3. Prior employment by the OSA; and/or
4. Family connection or close friendship with the OSA.

A COI:

1. Is the greatest threat to the impartiality in SCF CAP Ecosystem and associated activities;
2. Is a situation in which an individual has competing and incompatible relationships, obligations or affiliations with two different parties, in which the goals, aims or concerns of those parties are inherently at odds;
3. Can compromise good judgment and undermine trust and confidence in institutions and systems, including the SCF CAP; and
4. Arises when a participant's personal, financial or professional relationships compromise or appear to compromise their impartiality.

These types of relationships with the OSA would require disclosure, but depending on the particulars of each situation, they may or may not necessarily constitute a COI that could not be mitigated. Each COI situation is a specific use-case all its own with unique details and circumstances. The health of the SCF CAP Ecosystem relies on each member understanding what a COI is, what needs to be disclosed and how best it can be either mitigated or avoided.

DISCLOSURE AND MITIGATION

Disclosure and mitigation / avoidance of COI are critical to the success of SCF CAP. Without these, trust and confidence in the SCF CAP Ecosystem cannot be achieved.

Over the course of a career, modern professionals hold employment in numerous companies and organizations, invest in various business concerns, have families and develop scores of personal friendships. These can lead to COI. It is the failure to disclose a COI that runs afoul of responsible and ethical behavior.

The transparency of disclosed COI can insulate an individual, or organization, from scrutiny and potential charges of ethical misconduct.

MATERIAL VS NON-MATERIAL COI CONSIDERATIONS

To avoid any perception of COI, The Cyber AB's recommendation is to avoid any SCF CAP conformity assessments that have or allude to a COI between a 3PAO and the OSA. 3PAOs are responsible for developing, implementing and managing a capability for the 3PAO to identify potential instances of COI between its SCF Assessors and the OSA it is engaged in a contract with for SCF CAP conformity assessment services. The Cyber AB and SCF Council identify the minimum elapsed time necessary to avoid COI for 3PAOs and/or SCF Assessors:

3PAOs & SCF Assessors are prohibited from conducting 3PAAC Services if either the 3PAOs or SCF Assessor, made a material impact on the OSA's cybersecurity and data protection program. Materiality impact is defined as:

1. Material Impact - Within the past five (5) years, the 3PAO or SCF Assessor made a significant impact on the OSA's cybersecurity and/or data protection program, where the 3PAO or SCF Assessor performed a broad scope of work with a strategic and/or operational impact on the OSA's cybersecurity and/or data protection controls; and

2. Non-Material Impact - Within the past three (3) years, the 3PAO or SCF Assessor made no greater than a minor impact on the OSA's cybersecurity and/or data protection program, where the 3PAO or SCF Assessor performed a limited scope of work with minimal impact on tactical-focused cybersecurity and/or data protection controls.

Non-Material Impact

Pertaining to COI analysis, "non-material" means no greater than a minor impact on the organization's cybersecurity program that is categorized by a limited scope of work with a minimal impact on tactical-focused cybersecurity and/or privacy controls. Examples include, but are not limited to prior work with the OSA that involved:

1. Limited to suggesting improvements to the OSA's existing policies, standards and/or procedures;
2. Recommending, architecting and/or implementing technology that indirectly impacts the ISMS (e.g., security training, O365 licensing sales, etc.);
3. Tuning a Security Incident Event Manager (SIEM); and/or
4. Not related to performing an audits / gap assessments for the OSA, where the SCF Assessor's work was part of the audit / gap assessment team.

Material Impact

Pertaining to COI analysis, "material" means a significant impact on the organization's cybersecurity program that is categorized by a broad scope of work with a significant impact on strategic and/or operational-focused cybersecurity and/or privacy controls. Examples include, but are not limited to prior work with the OSA that involved:

1. Recommending, architecting, authoring and/or implementing policies, standards and/or procedures;
2. Recommending, architecting and/or implementing technology that directly impacts the ISMS (e.g., SIEM, ITAM, MFA, IAM, etc.);
3. Recommending, architecting and/or defining the scope of cybersecurity and/or privacy controls;
4. Acting as part of an audit / gap assessment team where the results of such activities were used to improve the ISMS; and/or
5. Acting as a "virtual CISO" or similar authoritative role.

Non-Certification Assessments

A non-certification assessment is the conduct by a 3PAO of a full or partial cybersecurity assessment of an OSA that does not result in the issuance or denial of a formal certification. Non-certification assessments are often referred to as "mock assessments," "gap assessments," or "dry-run assessments," among others. A non-certification assessment could involve the conduct by a 3PAO of a full or partial SCF CAP assessment or assessments of conformity to other standards (e.g., ISO/IEC 27001:2022).

A non-certification assessment does not result in the issuance of a SCF Certification, nor convey any standing within the SCF CAP. Non-certification assessments are conducted outside the purview of the SCF CAP and are not reported to The Cyber AB.

Some OSAs may elect for a 3PAO to conduct a non-certification assessment that will serve as the basis of a SCF CAP self-assessment reporting responsibility they may have. Others may choose a non-certification assessment to solicit a formal, structured third-party evaluation of the effectiveness of their SCF CAP implementation to date.

To be regarded as a true mock assessment that does not create a COI, the 3PAO must meet the following conditions:

1. The non-certification assessment must be conducted in a formal fashion and in accordance with the SCF CAP BoK and framework-specific SCF CAP conformity assessment Guide (AG).
2. The 3PAO must not provide any recommendations, advice or consultative information as to how the OSA might:
    a. Remediate any discrepancies; and/or
    b. Improve its security posture for:
        i. An official SCF CAP assessment; or
        ii. Any other cybersecurity standard;
3. The OSA must receive a deliverable that documents the official results of the non-certification assessment; and

4. The 3PAO must retain the results deliverables of all non-certification assessments conducted for the prior three (3) years. The results deliverables shall be made available to The Cyber AB, upon reasonable request, for purposes of review during a SCF CAP authorization renewal or accreditation assessment of the 3PAO by The Cyber AB.

APPENDICES

APPENDIX A: ENFORCEMENT

This Code of Professional Conduct (CoPC), essential to maintaining trust and confidence in the SCF CAP Ecosystem, will be actively enforced by The Cyber AB. The following procedures apply to the inquiry, review, adjudication and enforcement of the CoPC.

REPORTING VIOLATIONS

The Cyber AB monitors the SCF CAP-related activity of all SCF CAP authorized, accredited, certified, designated, approved and registered individuals and organizations within the Ecosystem and reserves the right to investigate any potential violations of this Code that arise from questionable behavior. In addition, the SCF Council plays a role in identifying and reporting potential violations that come to its attention.

The size and scale of the SCF CAP Ecosystem, however, presents challenges for The Cyber AB and SCF Council to effectively monitor all members and activities by themselves. All members of the SCF CAP Ecosystem are encouraged to engage in the "self-regulating" culture of the Program in furtherance of maintaining trust and confidence in the SCF CAP.

When observing other individuals or organizations within the SCF CAP Ecosystem making choices that may be in violation of the CoPC, interested parties should consider privately requesting clarification or offering to assist in rectifying the alleged violation. However, if clarification or resolution is not attainable or if an individual believes corrective action is required to resolve the situation, then the individual may submit a complaint report to The Cyber AB.

Reports of potential SCF CAP violations may be submitted to The Cyber AB by sending an email to complaints@cyberab.org.

INVESTIGATION AND ADJUDICATION

Upon receipt of a complaint or suggestion of a potential violation of the CoPC, The Cyber AB Compliance Officer will initiate a formal case designation and begin a fact-finding inquiry in accordance with its documented process for receiving, evaluating and rendering decisions on complaints.

The Cyber AB's formal Complaint Process is available on its website: https://cyberab.org.

Based on the complaint and subsequent fact-finding inquiry, the Compliance Officer will determine if a formal investigation of the matter is warranted. If a formal investigation is initiated, The Cyber AB will inform the SCF Council in writing of such within three (3) business days. The Compliance Officer will conduct a thorough investigation into the matter in accordance with procedures that provide notice to the accused, an opportunity to respond and review by unbiased decisionmakers with a right to appeal.

Upon completion of the investigation, the Compliance Officer will submit the results to The Cyber AB's Ethics and Compliance Committee of its Board of Directors. The Ethics and Compliance Committee will review the case file and determine if additional information is required. Upon final adjudication, the Ethics and Compliance Committee will render a decision on the validity of the original complaint and any penalties that might be imposed, pursuant to the complaint process.

The Cyber AB will report to the SCF Council in writing the outcome of completed investigations within fifteen (15) business days.

CORRECTIVE ACTION AND PENALTIES

The investigation may result in findings and recommendations for corrective action and/or penalties. Actions may include warning, remediation, suspension or denial or termination of SCF CAP credentials, as well as temporary or permanent loss of eligibility for such credentials. The Cyber AB and the SAICO have the sole authority to determine the action to be taken. In the event of termination of credentials, the termination will be conducted in accordance with the provisions of The Cyber AB's Complaint Process.

APPEALS

Individuals and organization subject to The Cyber AB's Ethics and Compliance Committee decisions will have twenty-one (21) days from the date of the report of the decision to file an appeal. Appeals will be received, considered and adjudicated in accordance with The Cyber AB's Appeals Process.

The Cyber AB Appeals Process is available on: https://cyberab.org.

APPENDIX B: CONFLICTS OF INTEREST (COI) EXAMPLE SCENARIOS

The information contained in this Appendix is supplemental guidance and not authoritative in nature. Nothing contained herein should be considered dispositive to any particular real-world SCF CAP situation, as the details of any discrete SCF CAP situation are unique. 3PAOs are reminded of their impartiality responsibilities under ISO/IEC 17020:2012.

The following situational examples of COI are:

1. Provided to illustrate and help clarify how various conflicts might be considered within the SCF CAP Ecosystem, along with their hypothetical resolution through mitigation or avoidance measures; and
2. Fictional, where any resemblance to actual companies or organizations, within the SCF CAP Ecosystem or outside, are purely coincidental:

COI EXAMPLE 1: FAMILIAL COI BETWEEN SCF ASSESSOR AND OSA

Scenario: Larry is a SCF Assessor affiliated with a 3PAO through a consulting agreement (e.g., 1099 contractor). An OSA contracts with Larry's 3PAO to conduct a SCF CAP conformity assessment. Coincidentally, Larry's brother, Darrel, is employed by the OSA as the deputy Chief Information Security Officer (CISO). Unaware of this relationship, the 3PAO assigns Larry to be a member of the assessment team for this SCF CAP conformity assessment.

Conflict: If Larry were to proceed with participating in this SCF CAP conformity assessment, his requirement for impartiality would conflict with his relationship with his brother. Left unmitigated, Larry's impartiality on the assessment would be compromised based on his likely sentiment for favoring a positive assessment outcome for Darrel and his company (or, in the event of a contentious brotherly relationship, possibly favoring a negative outcome).

Mitigation: When made aware of his assignment to be part of this assessment team, Larry discloses the COI to the 3PAO. Upon Larry's disclosure, the 3PAO mitigates the conflict by removing him from the assessment team for that 3PAO and replaces Larry with another SCF Assessor. Since there is no longer this or any other conflict in play, the 3PAO proceeds with the certification assessment.

Additional Discussion: Even if Larry qualified his disclosure that he and his brother had grown apart over the years due to them living on opposite coasts and that they had not seen or spoken with each other in years, the appearance of a COI would still exist and likely require similar mitigation on the part of the 3PAO.

COI EXAMPLE 2: CONSULTING COI BETWEEN 3PAO AND OSA

Scenario: A 3PAO had been providing consulting services and IT-related product sales while awaiting the results of its application to become a 3PAO. One of its product lines was a specialized set of SCF CAP-related documentation templates that assist companies in organizing their information and guides them through the implementation of cybersecurity and data protection requirements. Eighteen (18) months ago, the 3PAO sold a package of its documentation templates to an OSA, but did not provide any consulting services as the OSA was confident it could implement SCF CAP preparations on its own. At present, the OSA now wants to undergo a SCF CAP conformity assessment and contract with the 3PAO to perform the assessment.

Conflict: Even though the 3PAO did not provide any "traditional" (e.g., person-to-person) consulting services to the OSA, the provision of implementation templates, documentation or other tools that guide or assist a company in prioritizing, remediating or otherwise improving their understanding of SCF CAP requirements constitutes a form of advisory activity. Supplying these types of products to an OSA would compromise impartiality on a SCF CAP conformity assessment as the 3PAO would essentially be evaluating the effectiveness, accuracy and conformity of its own products.

Mitigation: The 3PAO understands the intrinsic COI in assessing an IT environment that was assisted or influenced by its own products. Since there is no measure that would mitigate the COI in this situation, the 3PAO concludes that this is a conflict that must be avoided. The 3PAO informs the OSA that they are unable to perform the SCF CAP conformity assessment themselves and refers the company to the SCF CAP Marketplace where other 3PAOs are listed for hire.

COI Example 3: Financial COI Between 3PAO and OSA

Scenario: Joanna is the Chief Operating Officer (COO) of a 3PAO. She is not a SCF Assessor, but she sits on the 3PAO's Appeals Committee. Long ago, at the advice of her financial advisor, she invested in a publicly traded company that designs and manufactures advanced avionics for both commercial and U.S. military aircraft. Her investment is in the form of direct ownership of the company's common stock. That same company has recently approached the 3PAO about conducting its SCF CAP conformity assessment. Joanna had previously disclosed her financial interest in this company as part of the 3PAO's internal COI disclosure program. When the 3PAO's compliance manager conducted the COI screening before taking on the new client, Joanna's disclosure was identified.

Conflict: The conflict exists between Joanna's financial interest in the avionics company and the 3PAO's responsibilities to conduct an impartial SCF CAP conformity assessment, including any potential appeal of the assessment results.

Mitigation: Since Joanna is not a SCF Assessor and is not directly involved in the 3PAO's cybersecurity compliance business line, there is no direct COI with the assessment team and this OSA. However, as COO, Joanna does sit on the 3PAO's Appeals Committee. The 3PAO mitigates this conflict by Joanna recusing herself from any involvement or influence in this particular OSA's assessment process or any potential appeal or complaint that might emerge from it. This recusal is documented by the 3PAO in a memorandum for the record and is retained as part of the assessment file for this OSA.

APPENDIX C: SCF CAP POSITION-SPECIFIC PROFESSIONAL RESPONSIBILITIES

Within the SCF CAP Ecosystem, individuals may hold multiple roles. Each role held by an individual, however, has position-specific professional and ethical requirements to which adherence is mandatory. Violating these requirements could result in referral to The Cyber AB and/or the SAICO for inquiry, review and adjudication, including the possible imposition of penalties.

SCF ASSESSORS

The following professional responsibilities apply to SCF Assessors:

1. Participate on a SCF CAP conformity assessment only under the direct employment, or contract (e.g., 1099), of a SCF 3PAO;
2. Complete SCF Assessor training as delivered only by an SCF Approved Training Provider (ATP) that utilizes SCF CAP Approved Training Materials (ATM);
3. Maintain up-to-date training and certification per SAICO requirements;
4. Render annual professional maintenance fees to the SAICO;
5. Sign annual renewal agreements with the SAICO;
6. Disclose all relevant COI, including where an appearance thereof may exist, to any company or organization employing or contracting you to participate in a SCF CAP assessment;
7. Refrain from knowingly and intentionally disseminating disinformation about the SCF CAP, other members of the SCF CAP Ecosystem, The Cyber AB and/or the SAICO;
8. Provide all documentation and records in English;
9. Do not share any SCF CAP assessment-related outcomes or advanced information with any person not assigned to that specific assessment, except as otherwise required by law;
10. Immediately notify the responsible 3PAO of any breach or potential breach of security to any SCF CAP-related assessment materials under the assessor's purview; and
11. Only use IT, cloud, cybersecurity services and end-point devices provided by the authorized / accredited 3PAO that has been engaged to perform that OSA's SCF CAP conformity assessment:
    a. Individual assessors are prohibited from using any other IT, including IT that is personally owned, to include internal and external cloud services and end-point devices, to process, store or transmit SCF CAP assessment reports or any other SCF CAP assessment-related information; and
    b. The evaluation of assessment evidence within the OSA environment, using OSA tools, is permitted.

SCF INSTRUCTORS

The following professional responsibilities apply to all SCF Instructors:

1. Provide formal SCF CAP course instruction only under the direct employment or contract of an Approved Training Provider (ATP). All ATPs must be approved by the SAICO;
2. Provide formal SCF CAP course instruction only for course levels for which you are qualified and certified (e.g., you cannot instruct a SCF Assessor course if you only hold a CCP certification);
3. Complete Instructor training as delivered only by the SAICO or an ATP;
4. Utilize officially Approved Publishing Partner (APP) curriculum "as is" in the delivery of SCF CAP professional certification course instruction and refrain from modifying the content;
5. Keep training and certification up-to-date based on evolving requirements from the SAICO;
6. Render annual professional maintenance fees to the SAICO;
7. Sign annual renewal agreements with the SAICO;
8. Disclose all relevant COI, including where an appearance thereof may exist, to any company or organization employing or contracting you to instruct formal SCF CAP professional certification courses;
9. Refrain from knowingly and intentionally disseminating disinformation about the SCF CAP, other members of the SCF CAP Ecosystem, The Cyber AB and/or the SAICO;
10. Provide all documentation and records in English;
11. Provide The Cyber AB and the SAICO with the most up-to-date and accurate information detailing their qualifications, training experience, professional affiliations and certifications and, upon reasonable request, submit documentation verifying this information;

12. Do not provide SCF CAP consulting services while serving as a SCF CAP instructor. This restriction prohibits the instructor from providing consulting services or offering targeted advice to students while in the act of providing classroom (in-person or virtual) instruction but does not necessarily prevent the instructor from providing consulting services as a separate professional activity outside the SCF CAP classroom;
13. Do not solicit consulting business or market any product or service while delivering SCF CAP training for an ATP;
14. Keep confidential all information obtained or created during the performance of SCF CAP training activities, including trainee records, except as required by law;
15. Notify The Cyber AB, or the SAICO, if required by law or authorized by contractual commitments to release confidential information; and
16. Do not share with anyone any SCF CAP training-related information not previously publicly disclosed.