SECURE CONTROLS FRAMEWORK

SCF CAP CERTIFICATION CHECKLIST

The Heartbeat of Compliance™

SCF ECOSYSTEM

The Secure Controls Framework (SCF) is a global leader in the field of cybersecurity and data protection controls. As a "framework of frameworks," the metaframework nature of the SCF covers over 200 laws, regulations and frameworks to provide unmatched breadth and depth coverage, including:

- Controls
- Control Weighting
- Assessment Objectives (AOs)
- Evidence Request List (ERL)
- Maturity Criteria
- Risk Catalog
- Threat Catalog

The SCF is free to use, since it leverages the Creative Commons licensing model. There are no expensive tool subscriptions – no strings attached. The mission of the SCF is to provide a powerful catalyst that will advance how cybersecurity and data protection controls are utilized at the strategic, operational and tactical layers of an organization, regardless of its size or industry.

The **Secure Controls Framework Conformity Assessment Program (SCF CAP)** is the certification methodology used to offer SCF-based certifications. The SCF CAP is designed to utilize tailored cybersecurity and data protection controls that specifically address the applicable statutory, regulatory and contractual obligations an Organization Seeking Assessment (OSA) is required to comply with. An OSA can obtain either:

- A single certification (e.g., CORE Fundamentals, NIST CSF 2.0, HIPAA Security Rule, etc.); or
- Multiple certifications as part of the same SCF assessment.

As the Accreditation Body (AB) for the SCF CAP, The Cyber AB governs the SCF Ecosystem. The key players in the SCF CAP include:

- **Organizations Seeking Assessment (OSA).** OSAs are organizations that are working towards earning a SCF-based certification, but have not yet undergone a SCF assessment.
- **Third-Party Assessment Organization (3PAO).** 3PAOs are entities accredited by The Cyber AB to conduct SCF-related Third-Party Assessment, Attestation, and Certification (3PAAC) services.
  - OSAs contract with a 3PAO to perform a SCF assessment.
  - 3PAOs employ SCF Assessors who are qualified to participate in and/or lead the SCF assessment.
  - SCF Assessors analyze SCF controls to determine if the control is appropriate, properly implemented and produces the desired results.
- **Registered Provider Organization (RPO).** RPOs are organizations that provide SCF-related professional services, including consulting and implementation.
  - RPOs assist organizations in preparing for assessments, streamlining SCF adoption, and ensuring alignment with cybersecurity and compliance objectives.
  - RPOs have demonstrated a commitment to professionalism and expertise in implementing the SCF within diverse business environments.

Earning a **SCF Certified™** conformity designation is meant to signify an accomplishment, rather than be viewed as a "participation ribbon" that has little practical value:

- A SCF certification provides a tangible measure of confidence that an organization's security, compliance and/or resilience claims are legitimate;
- As cybersecurity and data protection operations are multi-faceted, the SCF CAP is designed to ensure that assessed controls reflect the real-world requirements faced by the OSA from a statutory, regulatory and contractual perspective; and
- An assessment that only covers a part of an OSA's cybersecurity and privacy program results in an inaccurate and incomplete report on the OSC's overall security posture. The SCF CAP eliminates a false sense of security, compliance or resilience to stakeholders (e.g., partners, investors, etc.).

STEP 1. OBTAIN STAKEHOLDER SUPPORT

Everyone agrees that security is important, but there are some people less enthusiastic about being able to demonstrate secure practices through an assessment. Therefore, it is necessary to obtain stakeholder buy in due to the "multi-player" nature of assessments that require coordination, as well as resources and inter-department cooperation. Steps to success include:

- □ **Identify applicable requirements**. This involves defining all applicable cybersecurity and data protection laws, regulations and frameworks that are applicable to your organization. It defines "what right looks like" for your organization.
- □ **Familiarize yourself with the SCF and SCF CAP**. The SCF is a tool and like any tool, there is an expectation that users are familiar with how it is designed to work (e.g., a screwdriver is designed to function as a screwdriver, not a prybar). The SCF has a lot of free educational resources to set users up for success on how to maximize the use of the SCF, as well as how to obtain a SCF-based certification.
- □ **Choose your certification path**. Based on your knowledge of the organization, identify the most appropriate SCF Certification (e.g., CORE Fundamentals, NIST CSF 2.0, HIPAA Security Rule, etc.).
- □ **Identify internal stakeholders**. Identify the stakeholders and decision makers that you need to educate. Each will have their own interests, so meet with them to understand their goals and priorities related to secure, compliant and resilient operations.
- □ **Present a business case**. With the information you obtained from relevant stakeholder and their security, compliance and resiliency goals, it is time to present the business case for an SCF Certification to your identified decision makers. *(note – 3PAOs and RPOs can assist with building and presenting a business case for third-party certifications, since they clearly understand the costs vs benefits analysis).*

STEP 2. PREPARE FOR YOUR SCF ASSESSMENT

To prepare for an SCF assessment, your organization should first understand the SCF, the assessment methodologies that will be used and the environment you want to have assessed. To minimize confusion on scoping, the SCF CAP leverages the Unified Scoping Guide (USG) as the authoritative source to define scoping criteria. Steps to success include:

- □ **Seek professional assistance (optional)**. RPOs exist to help organizations design and build SCF-based cybersecurity capabilities, including implementing SCF controls. If you are in need of professional assistance, find an RPO on the SCF Marketplace that can provide professional services.
- □ **Define the assessment boundary**. This step involves scoping the assessment to the appropriate People, Processes, Technologies, Data & Facilities (PPTDF) that are applicable to the assessment.
- □ **Collect evidence**. The SCF assessment Guides (AGs) contain an Evidence Require List (ERL) that lists documentation artifacts that the 3PAO will expect the OSA to provide as part of the assessment.
- □ **Perform an internal gap assessment**. In Step 1, you identified the certification path you want to follow (e.g., CORE Fundamentals, NIST CSF 2.0, HIPAA Security Rule, etc.), so now you need to understand how well your organization conforms to those requirements. This entails performing a gap assessment, where you identify the state of your controls:
  - The SCF wants you to be successful and provides the "answers to test" in the form of the published SCF assessment guides for its available certifications.
  - You can use the official assessment guide to perform the internal gap assessment.
- □ **Implement remediation actions for missing / deficient controls**. This step depends on the existing maturity of your cybersecurity and data protection controls. To get to a state where there is sufficient evidence of due care and due diligence to demonstrate conformity, an OSA may require minimal remediation efforts or it may require extensive project management involvement. This is OSA-dependent, based primarily on the readiness to withstand external scrutiny.

Step 3. Validate Assumptions

The SCF CAP was designed to be efficient and cost-effective. This design relies significantly on the OSA to prepare reasonable evidence of due diligence and due care to clearly demonstrate how controls are addressed. This helps minimize back-and-forth questions between the OSA and the 3PAO's assessment team, therefore reducing time and labor-related costs. Steps to success include:

- □ **Build a RASCI matrix to understand stakeholder roles and responsibilities**. It is expected that organizations will leverage third-parties for technology infrastructure and/or services. However, there is a need to clearly understand how those External Service Providers (ESP) affect an OSA's cybersecurity and data protection controls. This is often addressed through building a RASCI matrix that defines responsibilities associated with individuals or teams:
    - Responsible - entity directly responsible for performing a task (e.g., control/process operator);
    - Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner);
    - Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task;
    - Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and
    - Informed - entity(ies) not involved in task execution but are informed when the task is completed.
- □ **Determine control inheritance**. The SCF CAP Body of Knowledge (BoK) covers the topic of control inheritance, so it is important to understand requirements for reasonable evidence from the entity that you are claiming control inheritance from.
- □ **Perform a readiness assessment**. This mock assessment is a "readiness review" that will provide you with a reasonable understanding of how prepared your organization is for a 3PAO to perform the actual SCF assessment. Using the applicable SCF assessment guide to perform a mock assessment; there are two ways to complete this step:
    - Use internal staff; or
    - Hire a RPO.
- □ **If necessary, remediate deficient controls**. At this point, there should not be any "missing controls," but there may be deficient controls. As long as the control is not determined to be a material control, as designated in the assessment guide, it is still possible to demonstrate conformity without perfection. The SCF CAP BoK contains detailed information on how to determine a passing score.
- □ **Gather evidence artifacts**. The assessment guides contain evidence artifacts that the 3PAO will request as part of an Evidence Request List (ERL), prior to the start of the assessment.
    - It is strongly recommended that OSA's start early by evidence that the 3PAO will request as part of the ERL, since that is published as part of the assessment guides.
    - To ensure a smoother and more efficient evaluation process, assistance with generating and/or reviewing evidence artifacts is available by contacting a SCF RPO or engaging the SCF community (e.g., SCF Discord server).

Step 4. Find An Assessment Partner

It is important for an OSA to interview 3PAOs, since every organization has a unique set of industry expectations, business processes and technologies. It is up to the OSA to find the 3PAO that best fits their needs. Steps to success include:

- □ **Formalize a First Party Declaration (1PD) that the OSA is ready to be assessed**. Phase 1 of a SCF assessment is for the OSA to self-attest:

  - An internal assessment was completed; and
  - The results of the internal assessment were sufficient to demonstrate conformity.
- □ **Interview 3PAOs**. The OSA is now ready to engage a 3PAO, so it is time to visit the SCF Marketplace and setup meetings with 3PAOs to interview them.
- □ **Contact a 3PAO to perform an assessment**. Once the OSA selects the 3PAO it wants to work with, the 3PAO will create a Statement of Work (SOW) and contract with the OSA to perform the assessment. The SOW between the OSA and 3PAO dictates how and when the assessment will be performed.

STEP 5. PERFORM THE ASSESSMENT

The 3PAO will assign at least two (2) SCF Assessors to an assessment team. Steps to success include:

- □ **Gain access to SCF Connect.** The cost of an SCF assessment includes access to SCF Connect, the SaaS-based tool used as the Single Source of Truth (SSOT) throughout the assessment process.
  - If the OSA is already using SCF Connect, the OSA just needs to invite the 3PAO into the OSA's existing SCF Connect instance.
  - If the OSA does not already have a SCF Connect account, the 3PAO will invite the OSA to be part of an assessment and that invitation will provide the OSA with access into an assessment-specific SCF Connect instance.
  - At the completion of the assessment, OSAs will have the option to continue using SCF Connect to demonstrate continuous monitoring of its cybersecurity program.
- □ **The 3PAO requests evidence artifacts from the OSA**. Prior to the start of the assessment, the 3PAO's assessment team will provide the OSA with an ERL that identifies necessary artifacts to provide sufficient evidence of due diligence and due care.
- □ **Schedule the assessment with the 3PAO**. Phase 2 of a SCF assessment is the 3PAO performing Third-Party Assessment, Attestation and Certification (3PAAC) services. This starts with coordination between the OSA and 3PAO to schedule the dates of the assessment.
- □ **Be assessed by the 3PAO**. The SCF Assessors will conduct the assessment activities in accordance with the SOW between the OSA and 3PAO.
  - The SCF assessment methodology is meant to be efficient and minimize any on-site time by the 3PAO's assessment team.
  - SCF Assessors utilize an examine, interview and test assessment methodology, so the intent is evidence submitted as part of the ERL can be used to address Assessment Objectives (AOs) through documentation examination.
  - It is important to note that clear, concise documentation can make the Examine process more efficient and this can decrease SCF Assessor-related labor costs.
  - For AOs that the 3PAO's assessment team cannot address through the Examine process, the 3PAO will:
    - Request clarification on provided evidence;
    - Interview stakeholders; and/or
    - Coordinate with the OSA to test processes, if necessary.
  - The 3PAO is expected to provide the OSA with daily/weekly back briefs (e.g., running status updates), per the SOW.

Step 6. Report Assessment Findings

The SCF CAP was designed for efficiency. Part of this structure is to leverage quality 3PAOs with competent, certified individuals. The 3PAOs leverage an internal Quality Control (QC) function that is independent from the assessment team. This speeds up the process of issuing a conformity designation, without sacrificing quality. Steps to success include:

- □ **3PAO performs a quality control review**. This step really depends on the existing state of your cybersecurity and data protection controls, since it may require minimal remediation efforts or more significant efforts.
- □ **3PAO issues a conformity designation**. Based on a decision following the QC review, the 3PAO will issue a conformity designation:
  - If the OSA demonstrates fulfillment of specified requirements, the OSA will be granted a SCF Certified™ certification that is valid for three (3) years from the certification date; and
  - If the OSA fails to demonstrate fulfillment of specified requirements, it will be refused a SCF Certified™ certification.

Step 7. Maintaining Conformity

Upon earning a SCF certification, there are annual requirements to perform internal assessments and correct deficiencies. At the end of the three (3) year certification period, the OSA is required to have a 3PAO perform an assessment to maintain status as a SCF certified organization. Steps to success include:

- □ **Annual reviews**. While a SCF certification is valid for a period of three (3) years, OSAs are required to perform an annual 1PD between 3PAO engagements:
  - Deficiencies identified in the 1PD have one hundred and eighty (180) days to be remediated; and
  - A failing 1PD in between an OSA's bi-annual (every three (3) years) 3PAAC engagements will result in the loss of the SCF Certified™ certification.

Maximizing The Value Of A SCF Certification

The SCF is focused on helping companies be secure, compliant and resilient. Earning a SCF Certification helps provide evidence of those efforts and that has value:

Ability To Demonstrate Conformity With Reasonable Security Practices

There is a need to demonstrate "reasonable" security practices. Having a SCF certification is proof that can be used to demonstrate reasonable security practices exist.

No technology or process can provide "absolute security" due to the limits of human certainty. This uncertainty exists in the lifecycle of every system, application and/or product and is often due to the constraints of:

- Cost;
- Schedule;
- Performance;
- Feasibility; and
- Practicality.

Trade-offs must be made across contradictory, competing and conflicting needs and limitations. However, these trade-offs must be optimized to achieve reasonable, or adequate, security that reflects a risk-based decision by stakeholders.

Risk & Threat Awareness Leads To Negligence Avoidance

The act of preparing for an assessment, undergoing the assessment and then maintaining the certification brings cybersecurity into the forefront. Based on awareness of applicable risks and threats, it can provide the necessary level of motivation for executive leadership to take cybersecurity and data protection seriously. This awareness can directly influence corporate culture to build a secure, compliant and resilient workforce and business.

Understanding applicable threats and the risks associated with those threats can lead to risk-informed decisions that can help an organization avoid claims of negligence.

Competitive Advantage

With Third-Party Risk Management (TRPM) gaining importance as part of broader Supply Chain Risk Management (SCRM) practices, there is clearly a competitive advantage to being able to demonstrate compliance with applicable laws, regulations and frameworks.

Many laws, regulations and frameworks do not offer the ability to obtain a certification (e.g., NIST CSF 2.0, NIST 800-161, etc.) and the SCF CAP provides a capability to provide assurance to stakeholders that an organization conforms with expected requirements.

This ability to demonstrate conformity can make your organization more attractive from a TRPM / SCRM perspective, due to minimized risk.