SECURE CONTROLS FRAMEWORK CONFORMITY ASSESSMENT PROGRAM (SCF CAP)

SUPPLEMENTAL GUIDANCE: APPLYING RECIPROCITY FROM CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) LEVEL 2 TO NIST CYBERSECURITY FRAMEWORK (NIST CSF) 2.0

version 1.0

This publication is available free of charge from: **https://securecontrolsframework.com/content/cap/ag-cmmc-l2-nist-csf-v-1-0.pdf**

Table of Contents

INTRODUCTION

This document is based on work by the Secure Controls Framework Council (SCF Council) specific to the:

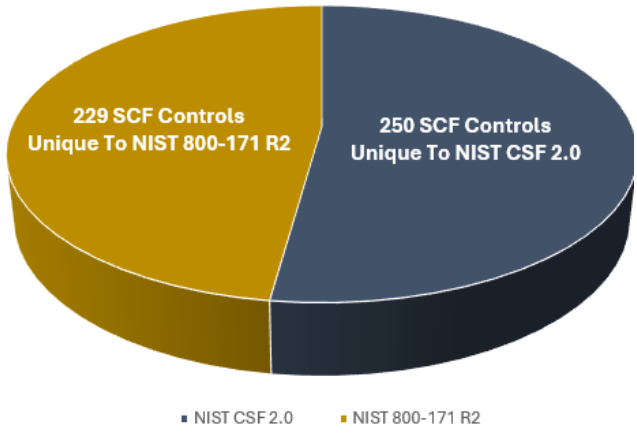
- Secure Controls Framework (SCF);[1]
- Secure Controls Framework Conformity Assessment Program Body of Knowledge (SCF CAP BoK); [2] and
- Security & Data Privacy Assessment Standards (CDPAS). [3]

CONTROL RECIPROCITY INTENT

This document is tailored for Organizations Seeking Assessment (OSA) that currently maintain Cybersecurity Maturity Model Certification (CMMC) Level 2 (L2) and want to earn a NIST Cybersecurity Framework (NIST CSF) certification, taking advantage of possible control reciprocity where applicable CMMC L2 controls could address NIST CSF controls, based on scoping and applicability.

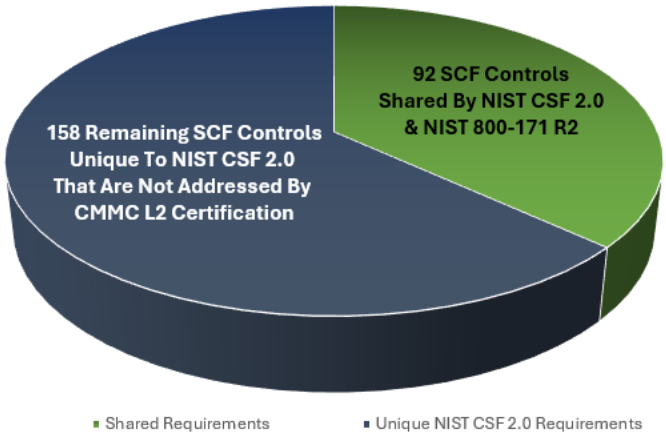
Leveraging Set Theory Relationship Mapping (STRM) used by the SCF:

- NIST SP 800-171 R2 has two-hundred twenty-nine (229) unique SCF controls; and
- NIST CSF 2.0 has two-hundred fifty (250 unique SCF controls.



Where NIST 800-171 R2 controls share scoping with NIST CSF 2.0 controls, reciprocity is acceptable. In an example where 100% reciprocity is permitted:

- NIST SP 800-171 R2 and NIST CSF 2.0 share ninety-two (92) SCF controls; and
- There are one-hundred fifty-eight (158) additional SCF controls that are unique to NIST CSF 2.0 that are not addressed by NIST SP 800-171 R2 (e.g., earning a CMMC L2 certification).



[1] *SCF – https://securecontrolsframework.com*
[2] *SCF CAP Body of Knowledge – https://securecontrolsframework.com/content/cap/scf-cap-bok.pdf*
[3] *SCF CDPAS – https://securecontrolsframework.com/content/cdpas.pdf*

Identified Coverage Gaps Between NIST CSF 2.0 and NIST SP 800-171 R2

Key areas of coverage in NIST CSF 2.0 that are not addressed by NIST SP 800-171 R2 include:

- Cybersecurity program oversight, including general Governance, Risk Management & Compliance (GRC) practices;
- Business integration of cybersecurity (e.g., defined mission, stakeholder expectations, compliance obligations, etc.);
- Disaster recovery and business continuity practices (e.g., Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), restoration activities, post-incident activities, etc.);
- Resource capacity management;
- A risk management program (e.g., priorities, ranking, constraints, risk tolerance, risk appetite, risk response, etc.);
- Supply chain risk management governance practices;
- Secure Software Development Practices (SSDP);
- Environmental threat protection (e.g., physical security, water damage, humidity controls, fire protection, etc.);
- Defined cybersecurity roles and responsibilities;
- Resource management to support cybersecurity initiatives;
- Measures of performance (e.g., metrics);
- Asset governance practices (e.g., hardware integrity, defined lifecycles; criticality, prioritization, etc.);
- Asset maintenance practices (e.g., preventative maintenance, reactive maintenance, etc.);
- Threat intelligence (e.g., insider threats, threat intelligence education, threat catalog, threat analysis, etc.);
- Continuing Professional Education (CPE) for cybersecurity personnel to maintain skills; and
- Incident response capabilities (e.g., chain of custody, escalation, reporting, etc.).

SCF Conformity Assessment Program (SCF CAP) Overview

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

The SCF Council established the Secure Controls Framework Conformity Assessment Program (SCF CAP) as a structure to conduct cybersecurity and data protection-related Third-Party Assessment, Attestation and Certification Services (SCF 3PAAC Services).[4] There is a need for a scalable, 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 exists to leverage SCF content to provide a company-level certification through a conformity assessment process. The SCF CAP is designed to make conformity assessments more cost-effective, efficient and objective through the use of the SCF's metaframework structure and no-cost content.

As a metaframework, the SCF CAP allows for a singular certification approach to cybersecurity & data protection requirements where it:

- Utilizes an examine, interview and test assessment methodology to demonstrate conformity with multiple requirements. This approach allows the SCF CAP to scale to cover multiple requirements simultaneously (e.g., demonstrate conformity with NIST CSF, HIPAA, EU GDPR, etc.) as part of a single assessment;
- Allows an organization to specify the statutory, regulatory and contractual obligations that are applicable to establish a Minimum Security Requirements (MSR) control set; and
- Leverages leading industry assessment practices to avoid "re-inventing the wheel" for assessment methodologies.

The SCF CAP:

- Is designed to produce a deliverable Report on Conformity (ROC) with a designation that summarizes the organization's overall cybersecurity & data protection program.
- Leverages concepts established in the CDPAS. [5]
- Can be scaled to provide conformity assessments for:
  - An entire organization;
  - A specific contract, project or initiative;
  - A specific Business Unit (BU) within an organization; or
  - A specific country, or geographic region, of the organization's business operations.

[4] *SCF CAP - https://securecontrolsframework.com/scf-conformity-assessment-program-cap/*

[5] *Cybersecurity & Data Privacy Assessment Standards (CDPAS) - https://securecontrolsframework.com/content/cdpas.pdf*

The SCF CAP BoK provides details on the SCF Certification process, including criteria necessary to obtain an SCF Certified™ certification. [6]

Third-Party Assessment, Attestation and Certification (3PAAC)

Third-Party Assessment, Attestation and Certification (3PAAC) addresses:

- Assessment: The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for an information system or organization. [7]
- Attestation: The issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated. [8]
- Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness. [9]

As part of SCF 3PAAC Services, a Third-Party Assessment Organization (SCF 3PAO) is expected to perform the following three (3) fundamental 3PAAC functions:

1. Conduct a conformity assessment of applicable cybersecurity and/or data protection controls within the OSA's assessment boundary;
2. Provide an attestation based on the findings from the conformity assessment in a Report on Conformity (ROC); and
3. Authorize the issue of a **SCF Certified™ - NIST CSF 2.0** certification, if sufficient conformity is achieved.

This document provides NIST CSF 2.0-specific conformity assessment guidance for conducting SCF 3PAAC Services, as part of the SCF CAP. An organization must achieve an assessment determination statement level of (1) Conforms or (2) Strictly Conforms to achieve status as **SCF Certified™ - NIST CSF 2.0**.

Normative References

The following normative references contain material that must be understood and used to utilize SCF 3PAAC Services to achieve status as **SCF Certified™ - NIST CSF 2.0**:

1. NIST Cybersecurity Framework (NIST CSF) version 2; [10]
2. NIST IR 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings*; [11]
3. Set Theory Relationship Mapping (STRM) – NIST CSF 2.0; [12]
4. STRM – NIST SP 800-171 R2; [13]
5. Cybersecurity & Data Protection Assessment Standards (CDPAS); [14] and
6. SCF Conformity Assessment Program Body of Knowledge (SCF CAP BoK). [15]

Intended Audience

The intended audience of this assessment guide is those parties that encompass the "assessment ecosystem," which includes:

- OSA;
- Third-Party Assessment Organizations (SCF 3PAOs);
- SCF Assessors; and

[6] *SCF CAP BoK – https://securecontrolsframework.com/content/cap/SCF CAP-BoK.pdf*
[7] *NIST Glossary for Assessment - https://csrc.nist.gov/glossary/term/assessment*
[8] *NIST Glossary for Attestation - https://csrc.nist.gov/glossary/term/attestation*
[9] *NIST Glossary for Certification - https://csrc.nist.gov/glossary/term/certification*
[10] *NIST CSF 2.0 download - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*
[11] *NIST IR 8477 - https://csrc.nist.gov/pubs/ir/8477/final*
[12] *SCF STRM for NIST CSF 2.0 - https://securecontrolsframework.com/content/strm/scf-strm-general-nist-csf-2-0.pdf*
[13] *SCF STRM for NIST CSF 2.0 - https://securecontrolsframework.com/content/strm/scf-strm-general-nist-800-171-r2.pdf*
[14] *CDPAS download - https://securecontrolsframework.com/content/cdpas.pdf*
[15] *SCF CAP BoK download - https://content.securecontrolsframework.com/scf-cap-bok.pdf*

- External Service Providers (ESP):
  - Consultants;
  - Cloud Service Providers (CSP);
  - Managed Service Providers (MSP); and
  - Managed Security Services Providers (MSSP).

The successful use of this document is predicated on an assumption that the reader has a baseline understanding of the:

- SCF's content; and
- SCF CAP's processes.

ASSESSMENT SCOPING

It is the OSA's responsibility to clearly identify CMMC L2 controls that are applicable to NIST CSF to streamline the conformity assessment process. In some situations, it may be possible to claim organization-wide reciprocity for nearly all CMMC L2 controls. However, in highly segmented CMMC environments, those CMMC L2 controls may only have narrow reciprocity (only applicable to those CMMC segments) and the organization would therefore be unable to claim organization-wide reciprocity.

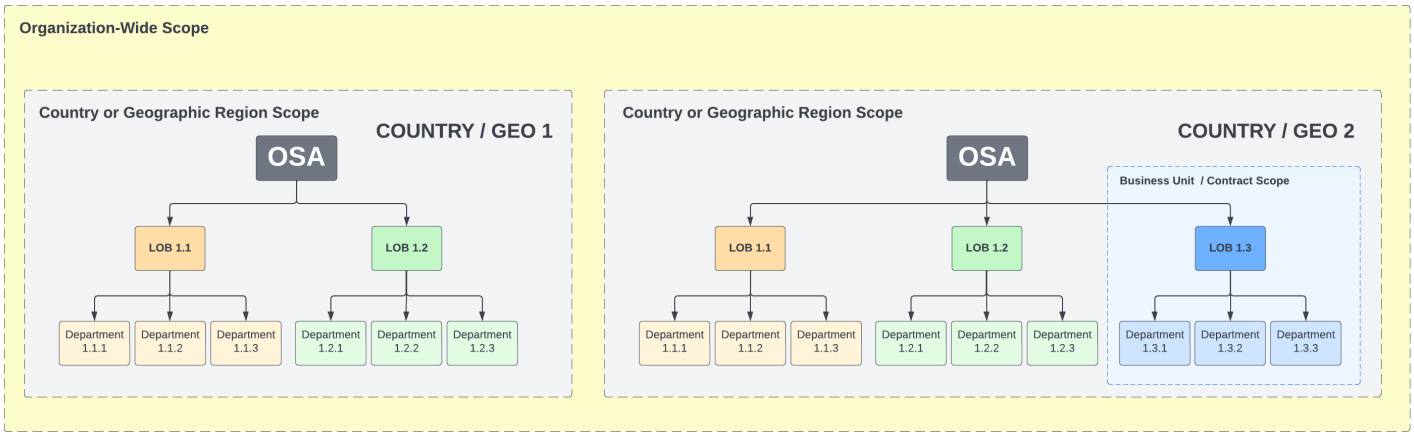
Prior to engaging with a SCF 3PAO for SCF 3PAAC Services, the OSA must specify the assessment scope. The assessment boundary demarcation can be defined as one (1) of the following four (4) scoping options:

1. Organization-wide;
2. A specific contract, project or initiative;
3. A specific Business Unit (BU) within the OSA; or
4. A specific country, or geographic region, of the organization's business operations.

To define the demarcation of the assessment boundary:

- For an organization-wide scope, it is defined by a discrete:
  - Taxpayer Identification Number (TIN);
  - Employer Identification Number (EIN);
  - Value Added Tax (VAT);
  - Dun & Bradstreet Data Universal Numbering System (DUNS); or
  - If applicable, a Commercial And Government Entity (CAGE) Code.
- For a contract, project, product or initiative, it is defined by:
  - Sufficient detail to describe the scope of the assessment boundary:
    - People;
    - Processes;
    - Technologies;
    - Data; and
    - Facilities;
  - Contract number and/or the name of the project or initiative; and
  - If applicable, a CAGE Code that is associated with the contract.
- For a BU, country or geographic region, it is defined by:
  - Sufficient detail to describe the scope of the assessment boundary:
    - People;
    - Processes;
    - Technologies;
    - Data; and
    - Facilities;
  - OSA-designated name for the BU, country(ies) or geographic region; and
  - If applicable, a CAGE Code that is associated with the BU.

A graphical representation of this assessment scoping is shown below:



The SFC Council recognizes the Unified Scoping Guide (USG) as the authoritative guidance for determining scope.[16]

UPDATES

Updates to the SCF CAP will be communicated via an advisory:

- Email notification (e-mail) to active SCF ecosystem stakeholders, including but not limited to:
  - SCF 3PAOs; and
  - SCF Assessors; and
- Blog posting on the SCF website for all others.

Errata will be provided to indicate:

- New content;
- Edited content; and/or
- Deleted/deprecated content.

When a new version of the SCF CAP or 3PAAC Guide & Standards is published, the previous version(s) is deprecated one hundred eighty (180) days after the release of the new version.

Additional SCF CAP-related guidance may be published to the SCF website (e.g., Frequently Asked Questions (FAQ)) without an advisory email notification or blog posting.

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

[16] *Unified Scoping Guide USG) - https://unified-scoping-guide.com*

CMMC L2 TO NIST CYBERSECURITY FRAMEWORK 2.0 CONTROLS

The SCF CAP provides two (2) formats of mappings:

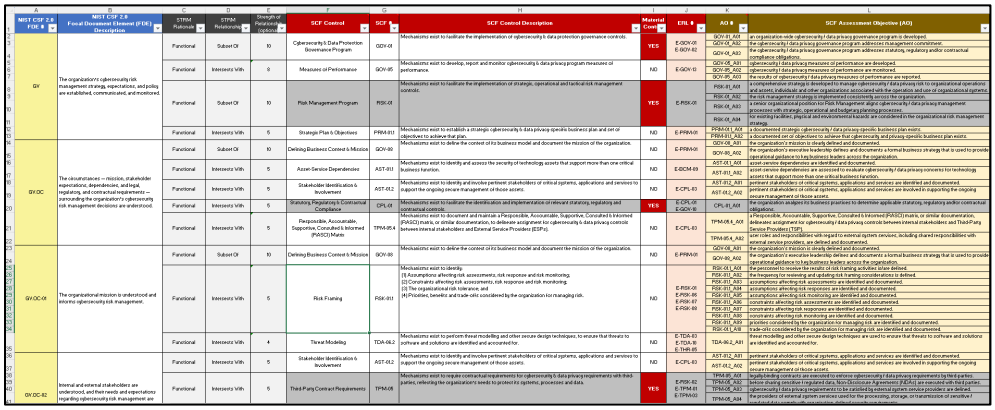
1. STRM formatted NIST CSF 2.0 to SCF.
2. SCF to NIST CSF (traditional SCF mappings); and

STRM is used to justify the mappings leveraged by the SCF for NIST CSF 2.0. The only difference is the formatting (e.g., perspective of the crosswalk mapping).

STRM - NIST CSF 2.0 TO SCF MAPPINGS

Annex 1 to the NIST CSF 2.0 Assessment Guide (scoped to address NIST SP 800-171 R2 control reciprocity):

- Contains the Set Theory Relationship Mapping (STRM) view of crosswalk mapping from NIST CSF 2.0 to SCF controls; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l2-delta-nist-csf-v-1-0.xlsx

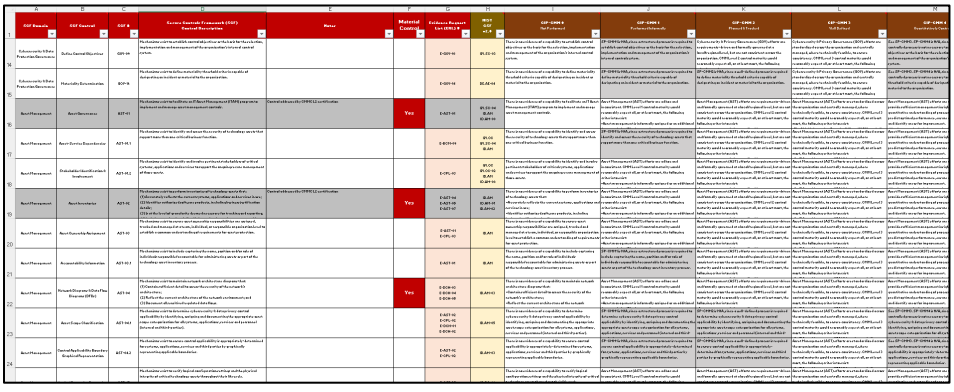


SCF TO NIST CSF 2.0 MAPPINGS

Annex 2 to the NIST CSF 2.0 Assessment Guide (scoped to address NIST SP 800-171 R2 control reciprocity):

- Contains crosswalk mapping from SCF to NIST CSF 2.0 controls; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l2-delta-nist-csf-v-1-0.xlsx
-

Note: The most efficient method of addressing NIST CSF 2.0 controls is through the format provided in Annex 2. The reason for this is it provides a significant reduction in duplication (e.g., SCF controls that address multiple NIST CSF functions). This is due to the high-level nature of the NIST CSF functions, categories and sub-categories.



ANNEXES

ANNEX 1: NIST CSF 2.0 TO SCF CROSSWALK MAPPING

Annex 1 to the NIST CSF 2.0 Assessment Guide:

- Contains the Set Theory Relationship Mapping (STRM) view of crosswalk mapping of NIST CSF 2.0 to SCF controls for NIST CSF 2.0 requirements that would not be possible of having reciprocity from CMMC 2.0; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l2-delta-nist-csf-v-1-0.xlsx

ANNEX 2: SCF TO NIST CSF 2.0 CROSSWALK MAPPING

Annex 2 to the NIST CSF 2.0 Assessment Guide:

- Contains crosswalk mapping from SCF to NIST CSF 2.0 controls for NIST CSF 2.0 requirements that would not be possible of having reciprocity from CMMC 2.0; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l2-delta-nist-csf-v-1-0.xlsx

Note: The most efficient method of addressing NIST CSF 2.0 controls is through the format provided in Annex 2. The reason for this is it provides a significant reduction in duplication (e.g., SCF controls that address multiple NIST CSF functions). This is due to the high-level nature of the NIST CSF functions, categories and sub-categories;

Annex 2 also contains complete listing of NIST CSF 2.0-specific Maturity Level Criteria (MLC). MLC are located on columns H through M on the Annex 2 tab of the Excel spreadsheet.

ANNEX 3: NIST CSF 2.0 ASSESSMENT OBJECTIVES (AOS)

Annex 2 to the NIST CSF 2.0 Assessment Guide:

- Contains a complete listing of SCF-based AOs for NIST CSF 2.0 requirements that would not be possible of having reciprocity from CMMC 2.0; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l2-delta-nist-csf-v-1-0.xlsx

Note: AOs are located on columns E on both the "Annex 1 – NIST CSF 2.0 to SCF" and "Annex 3 – NIST CSF 2.0 AOs" tabs of the Excel spreadsheet.

ANNEX 4: NIST CSF 2.0 EVIDENCE REQUEST LIST (ERL)

Annex 2 to the NIST CSF 2.0 Assessment Guide:

- Contains a complete listing of NIST CSF 2.0-specific evidence artifacts for NIST CSF 2.0 requirements that would not be possible of having reciprocity from CMMC 2.0; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l2-delta-nist-csf-v-1-0.xlsx

ANNEX 5: SCF CAP RASCI

Annex 5 to the NIST CSF 2.0 Assessment Guide:

- Contains a RASCI matrix for 3PAAC Services; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l2-delta-nist-csf-v-1-0.xlsx

ANNEX 6: 3PAAC DPIA TEMPLATE

Annex 2 to the NIST CSF 2.0 Assessment Guide:

- Contains a reference DPIA template that 3PAOs can use to assess data protection risks as part of 3PAAC Services; and

- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l2-delta-nist-csf-v-1-0.xlsx

ANNEX 7: MATERIALITY THRESHOLDS

Annex 7 to the NIST CSF 2.0 Assessment Guide:

- Contains a materiality threshold calculator that an OSA can use to determine its materiality threshold; and
- Is available to download from: https://securecontrolsframework.com/content/cap/annexes-cmmc-l2-delta-nist-csf-v-1-0.xlsx