Secure Controls Framework Conformity Assessment Program (SCF-CAP)

Body of Knowledge (BoK)

Demonstrating Cybersecurity & Data Privacy In Practice

Version 2023.6

Secure Controls Framework Council, LLC (SCF Council) & Secure Controls Framework Accreditation Body (SCF-AB)
© All Rights Reserved 2023.

Table of Contents

BACKGROUND INFORMATION ON THE SCF CAP 4
- WHO IS THE SCF-AB? 4
- WHAT IS THE SCF CAP? 4
- WHY IS THERE ANOTHER CERTIFICATION? 4
- HOW LONG IS AN OSC'S SCF CERTIFICATION VALID? 4
- WHERE DO I GO TO GET STARTED? 5
- SCF CAP PROCESS FLOW DIAGRAM 5

EXECUTIVE SUMMARY 6

SECURE CONTROLS FRAMEWORK CONFORMITY ASSESSMENT PROGRAM (SCF CAP) 7
- OBJECTIVE OF THE SCF CAP 7
- INTEGRATED CONTROLS MANAGEMENT (ICM) 8
  - *Minimum Compliance Requirements (MCR)* 8
  - *Discretionary Security Requirements (DSR)* 8
- ACCREDITATION SCHEME 9
  - *Accredited vs Non-Accredited Certifications* 9
  - *Manual & Automated Assessment Options* 9
- DEFINING SYSTEMS OF RECORD (SOR) & SINGLE SOURCE OF TRUTH (SSOT) 10
  - *Single Source of Truth (SSOT)* 10
  - *Systems of Record (SOR)* 10
- KEY TERMINOLOGY & DEFINITIONS 10
- SCF CAP USE CASES 11

LEVERAGING THE CONCEPT OF MATERIALITY TO DEFINE CONFORMITY 12
- CYBERSECURITY MATERIALITY 12
- ORGANIZATIONAL RISK TOLERANCE 12
  - *Low Organizational Risk Tolerance* 13
  - *Moderate Organizational Risk Tolerance* 13
  - *High Organizational Risk Tolerance* 14
- OBJECTIVITY 14
- CONFORMITY ASSESSMENT DESIGNATIONS 14
  - *Conforms* 14
  - *Significant Deficiency* 15
  - *Material Weakness* 15
- TRANSLATING RISK TOLERANCE TO SCF CAP ASSESSMENT RIGOR 15
  - *SCF CAP Level 1: Basic (Low Assurance)* 16
  - *SCF CAP Level 2: Focused (Moderate Assurance)* 18
  - *SCF CAP Level 3: Comprehensive (High Assurance)* 18

SCF CAP STRUCTURE 20
- CONFORMITY ASSESSMENT PRACTICES 20
- COMPENSATING CYBERSECURITY & DATA PRIVACY CONTROLS 21
- SCF CERTIFICATION PROCESS 21
  - *Phase 1 – First Party Declaration (1PD)* 21
  - *Phase 2 – Third-Party Assessment, Attestation & Certification (3PAAC)* 22

SCF CAP CERTIFICATION SCOPE 23
- ORGANIZATION VS BUSINESS UNIT 23
- DEFINING CONTROL APPLICABILITY 23
- UNIFIED SCOPING GUIDE (USG) 23

GLOSSARY 25
- ACRONYMS 25
- DEFINITIONS 25

APPENDIX A: ASSESSMENT RIGOR 27
- SCF CAP LEVEL 1: BASIC 27
- SCF CAP LEVEL 2: FOCUSED 29
- SCF CAP LEVEL 3: COMPREHENSIVE 31

APPENDIX B: REQUIREMENTS FOR CONFORMITY ASSESSMENT BODIES (3PAO) & SCF ASSESSORS 33
- SCF ASSESSOR CERTIFICATION REQUIREMENTS 33

DoD 8570-01 Certification Reciprocity *33*
Annual Registration Fee *33*
3PAO Sponsorship *33*
3PAO Accreditation **33**
Conflict of Interest (COI) Avoidance **34**
Appendix C: Understanding The Role of Security Mechanisms **35**
Adequate Security **35**
Secure Systems **36**
Stakeholder Security Requirements *36*
System Security Requirements *36*
System of Systems Mindset **36**
Appendix D: SCF Evidence Request List (ERL) **38**

BACKGROUND INFORMATION ON THE SCF CAP

WHO IS THE SCF-AB?

The Secure Controls Framework Accreditation Body (**SCF-AB**)[1] is a US-based, for-profit company that the Secure Controls Framework Council authorizes to operate an organization level cybersecurity & data privacy-specific conformity assessment process. The SCF-AB is governed by a board of advisors, consisting of recognized Subject Matter Experts (**SMEs**) within the cybersecurity & data privacy industries.[2]

WHAT IS THE SCF CAP?

The Secure Controls Framework Conformity Assessment Program (**SCF CAP**) is an organization-level conformity assessment. The SCF CAP is designed to utilize tailored cybersecurity & data privacy controls that specifically address the applicable statutory, regulatory and contractual obligations an Organization Seeking Certification (**OSC**) is required to comply with. By using the metaframework nature of the SCF, an OSC is able to perform a conformity assessment that spans multiple cybersecurity & data privacy-specific laws, regulations and frameworks.

Earning a **SCF Certified™** designation is meant to signify an accomplishment, rather than be viewed as a "participation ribbon" that has little practical value for the OSC or stakeholders in the OSC's supply chain to understand the OSC's security posture.

The SCF CAP is focused on using the SCF as the control set to provide a company-level certification. While the SCF-CAP shares some similarities with other existing, single-focused certifications (e.g., ISO 27001, CMMC, FedRAMP, etc.), the SCF CAP is unique in its metaframework approach to covering cybersecurity and data protection requirements that span multiple laws, regulations and frameworks.

WHY IS THERE ANOTHER CERTIFICATION?

Regardless of the industry, there is a definitive need for a third-party verified certification that assesses tailored cybersecurity & data privacy controls that could impact the OSC and its supply chain stakeholders. The SCF CAP was designed to deliver an organization-level certification that is industry-recognized, earned through a qualified third-party assessor's review of supporting evidence of a control's effectiveness.

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 OSC from a statutory, regulatory and contractual perspective. An assessment that only covers a part of an OSC's cybersecurity & data privacy program results in an inaccurate and incomplete report on the OSC's overall security posture, providing a false sense of security to the OSC.

The SCF CAP is designed for cybersecurity & data privacy practitioners by cybersecurity & data privacy practitioners. This concept is based on the need within the industry for a tailored conformity assessment solution that is capable of addressing several key considerations:

- View compliance as a natural by-product of secure practices;
- Scale to address multifaceted operational requirements (e.g., laws, regulations and frameworks);
- Acknowledge the stated risk tolerance of the OSC since not all organizations have the same risk tolerance;
- Minimize the risk of "gaming" the certification process that provides no useful insights into the security posture of the OSC;
- Utilize technology to make the assessment process more efficient to drive down labor-related assessment costs; and
- Leverage existing industry recognized practices, where possible.

HOW LONG IS AN OSC'S SCF CERTIFICATION VALID?

SCF Certification is valid for two (2) years from the date the OSC earns the SCF Certified™ designation, with the requirement for annual passing self-attestation through a First Party Declaration (**1PD**) to maintain the SCF Certified™ designation.

To become SCF Certified™, an OSC must successfully demonstrate appropriate evidence to a SCF Assessor, that works for a Third-Party Assessment Organization (**3PAO**). Only a 3PAO can issue the SCF Certified™ designation to an OSC.

---

*[1] Secure Controls Framework Accreditation Body (**SCF-AB**) – https://www.scf-ab.com*

[2] Please do not contact the SCF-AB to self-nominate for the SCF-AB Advisory Board since self-nominations are not accepted.

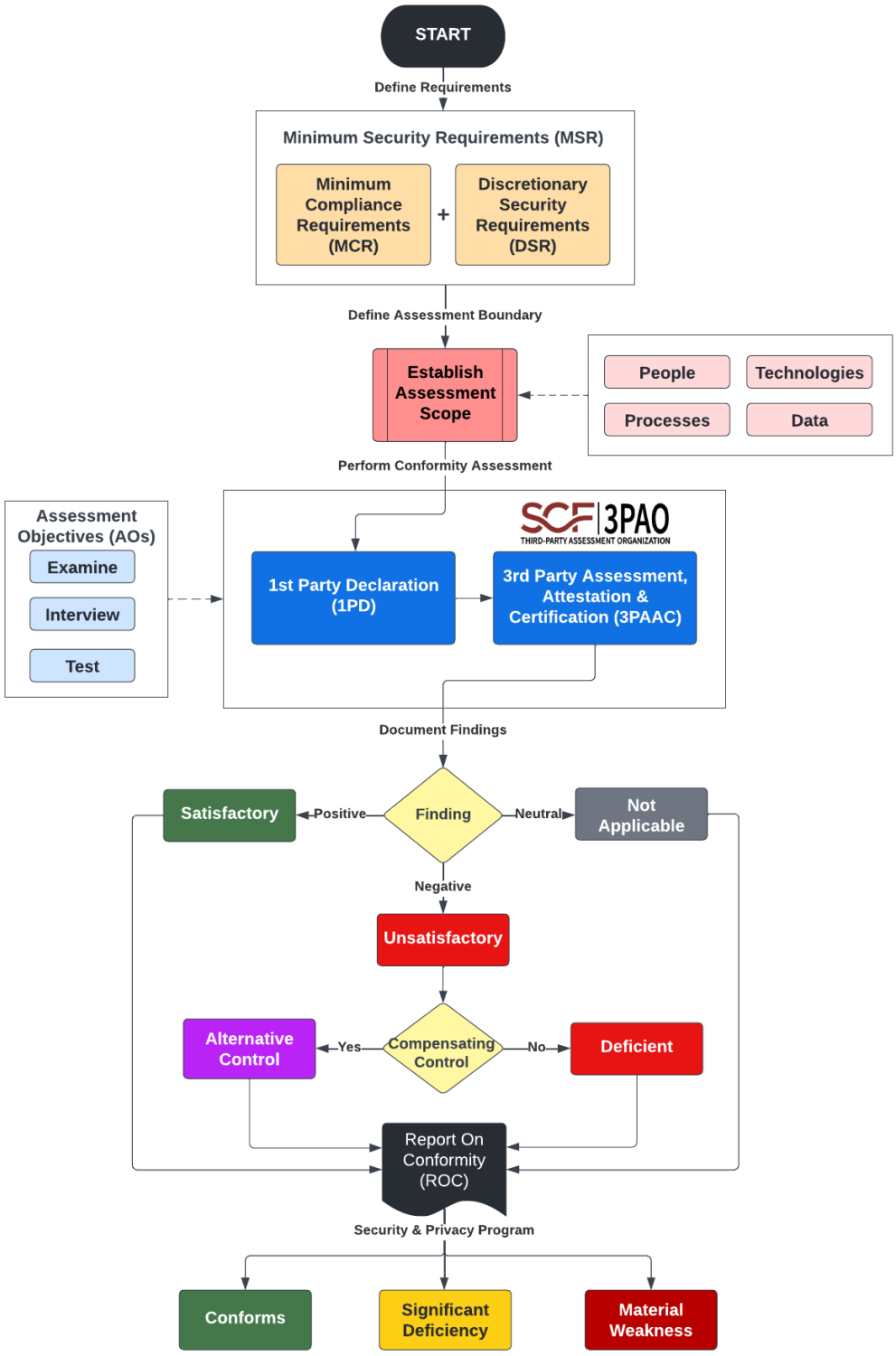
Where Do I Go To Get Started?

To get started, read this document to understand the SCF CAP and its supporting processes.

You can locate SCF-AB accredited 3PAOs on the SCF-AB's website. Prior to working with a 3PAO, the OSC is required to perform its own First-Party Declaration (**1PD**) that it has performed its own internal assessment. Assuming the OSC has appropriate evidence to support its 1PD, it is eligible to engage with a 3PAO for a third-party assessment. This is designed to manage expectations, so an OSC goes into a SCF assessment with a solid understanding of its control strength and available evidence to support its 1PD claims.

SCF CAP Process Flow Diagram

This graphic below shows a high-level process flow of the SCF CAP.



EXECUTIVE SUMMARY

The Secure Controls Framework (**SCF**) is a metaframework that consists of:

- Thirty-two (32) cybersecurity and data protection domains;
- Expert-derived crosswalk mapping to over 100 cybersecurity & data privacy-related laws, regulations and frameworks;
- Over 1,000 cybersecurity & data privacy-related controls;
- A six (6) level Capability Maturity Model (**CMM**) with defined maturity criteria for each control;[3]
- A risk catalog; and
- A threat catalog.

The SCF is designed to be a "Rosetta Stone" of cybersecurity & data privacy requirements that can enable:

- Intra-Organization Standardization. Cybersecurity, privacy, technology, Program Management (**PM**) and other stakeholders within an organization can utilize a single control set for their strategic, operational and tactical cybersecurity & data privacy-related controls; and
- Inter-Organization Standardization. Organizations can "speak the same language" for cybersecurity & data privacy-related controls, regardless of the industry vertical, geographic region and/or language.

The Secure Control Framework Conformity Assessment Program (**SCF CAP**) is specifically designed to:

- Provide a scalable approach to normalize requirements from multiple, disparate statutory, regulatory and contractual frameworks that can be assessed according to granular Assessment Objectives (**AOs**);
- Operationalize a third-party assessment model that leverages the metaframework approach of the SCF;
- Minimize the "gamification" of the cybersecurity & data privacy assessment process, to provide an assessment that accurately reflects the current state of an organization's cybersecurity and data protection (e.g., privacy) controls; and
- Provide a concise, easily-understood approach to reporting assessment status to various stakeholders.

The concept of the SCF CAP was to develop an assessment methodology "*by cybersecurity & data privacy professionals, for cybersecurity & data privacy professionals*" that objectively and accurately reflects the current state of an organization's cybersecurity & data privacy program. Earning a "SCF Certified™" certification is meant to signify an accomplishment, rather than an activity performed to "check the box" as part of a futile compliance exercise.

The CAP is designed to produce a deliverable Report on Conformity (**ROC**) with a designation that summarizes the organization's overall cybersecurity & data privacy program. Those three (3) possible designations are:

CONFORMS

A ROC designation of "Conforms" is a positive outcome. This indicates that the organization's cybersecurity & data privacy practices conform to its selected cybersecurity & data privacy practices. At the control level, there may be one or more deficient controls, but as a whole, the cybersecurity & data privacy practices support the organization's stated risk tolerance.

SIGNIFICANT DEFICIENCY

A ROC designation of "Significant Deficiency" is a negative outcome. This indicates cybersecurity & data privacy practices fail to support the organization's stated risk tolerance. Due to systemic problems in the cybersecurity and/or privacy program, there is insufficient evidence of due care and due diligence to provide assurance that the organization's stated risk tolerance is achieved.

MATERIAL WEAKNESS

A ROC designation of "Material Weakness" is a negative outcome. This indicates the organization is unable to demonstrate conformity with its selected cybersecurity & data privacy practices, due to material weaknesses that make it improbable that reasonably expected threats will be prevented or detected in a timely manner. This can directly, or indirectly, affect assurance that the organization can adhere to its own stated risk tolerance.

When an organization goes through a form of certification process, it undergoes a conformity assessment (e.g., ISO 27001, CMMC, SOC 2 Type 1, PCI DSS, RMF, etc.). Conformity assessments are designed to assure that a particular product, service or system meets a given level of quality or safety. Instead of 100% pass criteria, conformity assessments rely on an established, risk-based threshold to determine if control objectives have been achieved.

[3] *Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) - https://securecontrolsframework.com/capability-maturity-model/*

SECURE CONTROLS FRAMEWORK CONFORMITY ASSESSMENT PROGRAM (SCF CAP)

The Secure Controls Framework (**SCF**) is a comprehensive catalog of controls architected to enable organizations to design, build and maintain secure processes, systems and applications. The SCF addresses cybersecurity & data privacy, with the idea that these principles are "baked in" at the strategic, operational and tactical levels. The SCF's mission is to provide a powerful tool and methodology that will advance how cybersecurity & data privacy controls are implemented and assessed at an organization's strategic, operational and tactical layers, regardless of its size or industry.

The Secure Control Framework Conformity Assessment Program (**SCF CAP**) is authorized by the Secure Controls Framework Council (**SCF Council**) to promote transdisciplinary cybersecurity & data privacy competency for an Organization Seeking Certification (**OSC**). This concept of competency is focused on an OSC's ability to:

- Establish the context of its cybersecurity & data privacy program (e.g., applicable statutory, regulatory and contractual obligations);
- Define appropriate cybersecurity & data privacy controls from the SCF;
- Assign maturity-based criteria of selected cybersecurity & data privacy controls;
- Assign stakeholder accountability for the execution of assigned cybersecurity & data privacy controls; and
- Demonstrate evidence that due diligence and due care have been exercised in implementing cybersecurity & data privacy controls that satisfy the targeted maturity criteria.

The SCF CAP is focused on using the SCF as the control set to provide a company-level certification. While the SCF-CAP shares some similarities with other existing, single-focused certifications (e.g., ISO 27001, CMMC, FedRAMP, etc.), the SCF CAP is unique in its metaframework approach to covering cybersecurity and data protection requirements that span multiple laws, regulations and frameworks.

OBJECTIVE OF THE SCF CAP

There is a need for a scalable, cost-effective solution to obtain a company-level, third-party assessment of cybersecurity & data privacy practices. The SCF CAP is a means to make certification processes more cost-effective, efficient and objective. One strength of the SCF CAP is that the certification process is built by cybersecurity & data privacy subject matter experts to help enable cybersecurity & data privacy practices that can be properly assessed in context and scope.

Instead of "making a square peg fit into a round hole," the SCF CAP allows an organization to tailor its control set to meet its specific needs to demonstrate adherence to selected cybersecurity & data privacy controls. The resulting documentation of an assessment's findings will be presented in two (2) formats as part of the Report on Conformity (**ROC**):

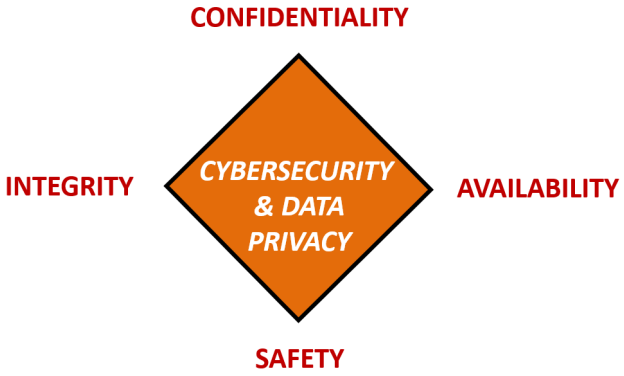
1. Technical Assessment Report (**TAR**) – full reporting that is not meant to be shared externally since it may contain sensitive controls information that are meant for internal audiences only.
2. Sharable Assessment Report (**SAR**) – ideal for sharing with clients and other third-parties.

As a metaframework, the SCF CAP allows for a "single certification" approach to cybersecurity & data privacy requirements:

- Enables an "*examine, interview and test once to demonstrate conformity with multiple requirements*" approach that will allow the SCF CAP to scale to cover multiple requirements simultaneously (e.g., demonstrate conformity with NIST CSF, ISO 27002, CCPA, EU GDPR, etc. as part of a single assessment);
- Will allow an organization to specify the statutory, regulatory and contractual obligations that are applicable to establish a Minimum Security Requirements (**MSR**) control set; and
- Leverages several leading practices to perform assessments to avoid "re-inventing the wheel."

INTEGRATED CONTROLS MANAGEMENT (ICM)

Regardless of industry, it is important for organizations to understand the difference between "compliant" versus "secure" since it is necessary to enable rational risk management discussions. This concept is increasing in importance as Cybersecurity Supply Chain Risk Management (**C-SCRM**) concerns drive cybersecurity & data privacy requirement definitions. Organizations need to demonstrate "security and privacy in practice" not only within their operations, but across the supply chain for third-party organizations that directly or indirectly affect the Confidentiality, Integrity, Availability and Safety (**CIAS**) of those affected systems, applications and/or services.



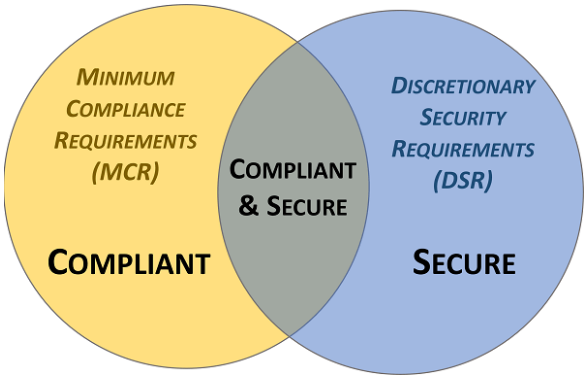
- *CONFIDENTIALITY* addresses preserving authorized restrictions on access and disclosure to authorized users and services, including protecting personal privacy and proprietary information.
- *INTEGRITY* addresses guarding against improper modification or destruction, including ensuring non-repudiation and authenticity.
- *AVAILABILITY* addresses timely, reliable access to data, systems and services for authorized users.
- *SAFETY* addresses reducing risk associated with technologies that could fail or be manipulated by nefarious actors to cause death, injury, illness, damage to or loss of equipment.

When evaluating appropriateness for cybersecurity & data privacy controls that apply to an application, service or process, not only should the organization's Governance, Risk Management and Compliance (**GRC**) personnel be involved, but business and process stakeholders should help identify "must have" vs "nice to have" requirements as part of Integrated Controls Management (**ICM**).

Minimum Security Requirements (**MSR**) are required to be defined by the OSC. The MSR is a combination of: [4]

- Minimum Compliance Requirements (**MCR**); and
- Discretionary Security Requirements (**DSR**).

From a business perspective, the combination of MCR and DSR identifies a Minimum Viable Product (**MVP**) for cybersecurity & data privacy protection measures. MSR are applicable for the application, service or process throughout its lifecycle. Developers and architects should strive for a set of cybersecurity & data privacy controls that equates to "secure and compliant" instead of just "compliant" as meeting minimum compliance requirements rarely means an application, service or process will be secure.



Minimum Compliance Requirements (MCR)

- These are the absolute minimal requirements that must be met to comply with applicable laws, regulations and contracts.
- MCR are primarily externally-influenced, based on industry, government, state and local regulations.
- MCR should never imply adequacy for secure practices and data protection since they are merely compliance-related.

Discretionary Security Requirements (DSR)

- These are tied to the organization's risk appetite as DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity and data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance.
- While MCR establish the minimal controls that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

The SCF CAP focuses on the Organization Seeking Certification (**OSC**) to define its MSR, according to applicable MCR and DSR criteria:

- The controls defined as MSR constitute the scope of the controls for the SCF CAP; and
- Based on the MSR, applicable Assessment Objectives (**AOs**) for those SCF controls will be used to evaluate control implementation.

[4] *Integrated Controls Model (ICM) - https://securecontrolsframework.com/integrated-controls-management/*

ACCREDITATION SCHEME

Conformity assessments serve as a method to determine whether a product, service or system meets the requirements of a particular standard. In the context of the SCF-CAP, the "standard" is the tailored SCF control set (e.g., Minimum Security Requirements). The SCF CAP serves as independent verification and confirms, through the examination of objective evidence, that specified requirements have been fulfilled.

For the accreditation scheme of the SCF CAP:

- The Secure Controls Framework Council (**SCF Council**) maintains the SCF and is independent from the SCF Accreditation Body (**SCF-AB**);
- The SCF Council is the scheme owner that provides criteria for the SCF-AB to implement and govern;[5]
- The SCF-AB is the Accreditation Body (**AB**) for the SCF CAP;
- The SCF-AB will accredit Certifying Bodies (**CB**) to perform conformity assessment activities (Third-Party Assessment, Attestation & Certification (**3PAAC**) Services);
    - The CB is also referred to as a 3rd Party Assessment Organization (**3PAO**); and
    - Accreditation is the process of evaluating the competence of a 3PAO;
- Only accredited 3PAOs will be allowed to perform 3PAAC Services;
- Organizations Seeking Certification (**OSC**) are the organizations undergoing an assessment and will independently hire a 3PAO to perform 3PAAC Services that covers the OSC's defined scope of certification;
- Based on a decision following Quality Assurance (**QA**) review, the 3PAO will issue an independent attestation of the OSC that fulfillment of specified requirements (e.g., Assessment Objectives (**AOs**)) has been demonstrated:
    - If the OSC demonstrates fulfillment of specified requirements, the OSC will be granted SCF Certified™ status; and
    - If the OSC fails to demonstrate fulfillment of specified requirements, it will be refused status as SCF Certified™; and
- The 3PAO will assign **SCF Assessors** under a Team Leader (**TL**) who is given the overall responsibility for the management of 3PAAC Services:
    - The TL will leverage 3PAO-provided Technical Experts (**TE**), working under the responsibility of a TL, to provide specific knowledge or expertise with respect to the scope of accreditation to be assessed; and
    - TEs do not assess independently.

Accredited vs Non-Accredited Certifications

Only a SCF-AB accredited CB can provide 3PAAC Services. In terms of the SCF CAP:

- An "accredited certification" is a valid SCF Certification that was performed by a SCF-AB accredited CB;
- A "non-accredited certification" is an illegitimate SCF Certification, performed by an organization that lacks designation as a SCF-accredited CB:
    - Non-accredited SCF Certifications are invalid;
    - Use of the term "SCF Certified™" by an organization not certified by a SCF-AB accredited CB infringes on the trademark of "SCF Certified™" and is subject to legal remedies; and
    - Performing 3PAAC Services by an organization that the SCF-AB does not accredit infringes on the trademark of "SCF Certified™" and is subject to legal remedies.

Manual & Automated Assessment Options

A 3PAO has three (3) methods available to perform 3PAAC services:

1. **Manual Point In Time (MPIT)** – MPIT is a traditional assessment methodology that relies on the manual review of OSC-provided artifacts to derive a finding that is relevant to a specific point in time (time at which the control was evaluated).
2. **Automated Point In Time (APIT)** – APIT utilizes automation to augment the traditional assessment methodology, where data feeds are evaluated for conformity through the aide of Artificial Intelligence and/or Machine Learning (AI/ML). Where technology cannot evaluate evidence, OSC-provided artifacts are manually evaluated to derive a finding. Both automated and manual evidence reviews are relevant to a specific point in time (time at which the control was evaluated).
3. **Automated Evidence with Human Assessment (AEHA)** – AEHA uses software-based logic to compare the desired state of security compliance vs current state of configuration and procedural controls. The relies on automated evidence (where technically possible to produce) with human/manual assessment practices to evaluate the evidence. This is a hybrid approach the leverages both automation technologies and human subject matter expertise.

[5] *"Scheme Owner" definition - https://csrc.nist.gov/glossary/term/scheme_owner*

Defining Systems of Record (SOR) & Single Source of Truth (SSOT)

Due to the complex nature of Integrated Controls Management (**ICM**), the SCF-AB determined that the Single Source of Truth (**SSOT**) for an Organization Seeking Certification (**OSC**) will be the SCF Connect tool.[6] SCF Connect is a cost-effective platform that is specifically designed to efficiently manage an organization's SCF-based ICM program.

Single Source of Truth (SSOT)

A Single Source of Truth (**SSOT**) refers to the practice of consolidating authoritative data in a single location. The SSOT is an aggregation of data from multiple data sources. The intent is to make an SCF Assessment as efficient and cost-effective as possible by presenting an SCF Assessor with necessary evidence in a format that saves both time and money for the OSC.

SCF Connect serves as the SCF-AB's officially-recognized tool for performing an SCF Assessment.

Systems of Record (SOR)

Systems of Record (**SOR**) are authoritative sources of specific types of data. For example:

- A Governance Risk & Compliance (**GRC**) solution is a SOR for policies & standards;
- A Security Incident Event Manager (**SIEM**) is a SOR for security event logs;
- An antimalware solution is a SOR for malware-related protection information;
- An IT Asset Management (**ITAM**) solution is a SOR for hardware and software management; and
- A Configuration Management Database (**CMDB**) solution is a SOR for system configurations and change management.

The SCF CAP's approach is for multiple SORs to feed evidence to the SOT through automated means or manual reporting.

Key Terminology & Definitions

Conformity assessments are commonly defined as the demonstration that specified requirements for a product, process, system, person or body are fulfilled. In summary:

- Accreditation is a third-party attestation of a conformity assessment body's demonstrated competence to carry out specific conformity assessment tasks;
- Certification is third-party attestation related to products, processes, systems or persons; and
- Attestation is the issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated.

The following terminology leveraged by the SCF CAP is based on the glossary of NIST Special Publication 2000-01, *ABC's of Conformity Assessment*:[7]

Industry-Defined Terminology	CAP-Specific Terminology	Definition	NIST-Referenced Source
Conformity Assessment	SCF Conformity Assessment (**SCA**)	Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.	ISO/IEC 17000
Certification	SCF Certification	Third-party attestation related to products, processes, systems or persons.	ISO/IEC 17000
Certification Body	SCF 3rd Party Assessment Organization (**3PAO**)	Third-party conformity assessment body operating a certification scheme (e.g., SCF CAP).	ISO/IEC 17065
Accreditation	3PAO Accreditation	Third-party attestation related to a conformity assessment body conveying a formal demonstration of its competence to carry out specific conformity assessment tasks.	ISO/IEC 17000
Accreditation Body	SCF Accreditation Body (**SCF-AB**)	The authoritative body that performs accreditation.	ISO/IEC 17000
Scheme Owner [program owner]	Secure Controls Framework Council, LLC (**SCF**)	Person or organization that is responsible for developing and maintaining a specific product certification scheme.	ISO/IEC 17067

[6] *SCF Connect - https://scfconnect.com/*
[7] *NIST SO 2000-01 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.2000-01.pdf*

Attestation	Report on Conformity (**ROC**)	Issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated. *Note: The resulting statement, referred to in this International Standard as a "statement of conformity", conveys the assurance that the specified requirements have been fulfilled.*	ISO/IEC 17000
Assessment Body	SCF 3rd Party Assessment Organization (**3PAO**)	The body that performs conformity assessment services.	ISO/IEC 17000
Specified Requirement	SCF Assessment Objective (**AO**)	Need or expectation that is stated.	ISO/IEC 17000
Certification Requirement	SCF Certification Requirement (**SCR**)	Specified requirement, including product requirements, are fulfilled by the client as a condition of establishing or maintaining certification.	ISO/IEC 17065 ISO/IEC 17021-1 ISO/IEC 17024
Declaration	First Party Declaration (**1PD**)	First-party attestation.	ISO/IEC 17000
First-Party Conformity Assessment Activity	First Party Conformity Assessment Activity (**1PCAA**)	Informal, internal conformity assessment activity that is performed by the person or organization that provides first-party attestation.	ISO/IEC 17000
Third-Party Conformity Assessment Activity	Third-Party Assessment, Attestation & Certification (**3PAAC**) Services	Conformity assessment activity that a person, or a body, performs that is independent of the person or organization that provides the object and of user interests in that object.	ISO/IEC 17000
Supplier Declaration of Conformity	Supplier Declaration of Conformity (**SDoC**)	Supplier declaration of conformity first- party attestation (e.g., 1PCAA) by an organization in the supply chain.	ISO/IEC 17050

SCF CAP Use Cases

Use cases for the SCF CAP include, but are not limited to an organization's:

- Desire by its executive leadership team to obtain an objective evaluation of its cybersecurity & data privacy program;
- Need to demonstrate "reasonably secure practices" to its:
  - Clients;
  - Industry partners (e.g., prime contractors);
  - Cybersecurity insurance underwriters; and
  - Other stakeholders; and
- Cybersecurity Supply Chain Risk Management (**C-SCRM**) practices that compel its subcontractors to obtain an objective evaluation so that it can evaluate risks associated with its direct supply chain.

The SCF CAP is designed to be a beneficial company-level certification that is earned, not purchased. Given the rigor of the SCF CAP, this means not all organizations undergoing an assessment will pass. However, the saying, "*Bad news is good news if you know what to do with it!*" applies to assessment results, where cybersecurity, IT and privacy leaders can successfully leverage the results from a "failed assessment" to their advantage to:

- Obtain necessary resources to remediate deficiencies; and
- Appropriately transfer risk to stakeholders for resourcing and remediation efforts.

LEVERAGING THE CONCEPT OF MATERIALITY TO DEFINE CONFORMITY

The SCF Council and SCF-AB recognize the concept of materiality as the means to determine a "pass or fail" designation for First Party Declaration (**1PD**) and Third-Party Assessment, Attestation & Certification (**3PAAC**) activities.

In order to determine a "pass or fail" designation to an assessment, when viewing an organization's conformity to a set of cybersecurity & data privacy controls, the SCA CAP focuses on the concept of materiality. There are several ways "materiality" is defined, based on the industry.[8] Specific to cybersecurity and data protection, the SCF defines a material weakness as:

> *"A deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data protection controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance."*

CYBERSECURITY MATERIALITY

Controls are the nexus of a cybersecurity & data privacy program, so it is vitally important to understand how controls are viewed from a high-level risk management perspective regarding "cybersecurity materiality" and the governance of an organization's cybersecurity & data privacy controls.

To better understand cybersecurity materiality, it is important to define specific risk management terminology. According to the PMBOK™ Guide:[9]

- Risk Tolerance is the "*specified range of acceptable results.*"
- Risk Threshold is the "*level of risk exposure above which risks are addressed and below which risks may be accepted.*"
- Risk Appetite is the "*degree of uncertainty an organization or individual is willing to accept in anticipation of a reward*." It is important to note that risk tolerance and risk appetite are not the same thing.

The concept of materiality helps provide an organization better understand the health of its cybersecurity & data privacy program, where a material weakness might expose systems, applications, services, personnel, the organization or third-parties to unacceptable risk. In addition, materiality designations can help determine what constitutes reasonable assurance that an organization adheres to its stated risk tolerance.

In the context of the SCF CAP, the risk tolerance is categorized according to the Assurance Level (**AL**)

1. Low Assurance – this corresponds to "high risk tolerance"
2. Moderate Assurance – this corresponds to "moderate risk tolerance"
3. High Assurance – this corresponds to "low risk tolerance"

ORGANIZATIONAL RISK TOLERANCE

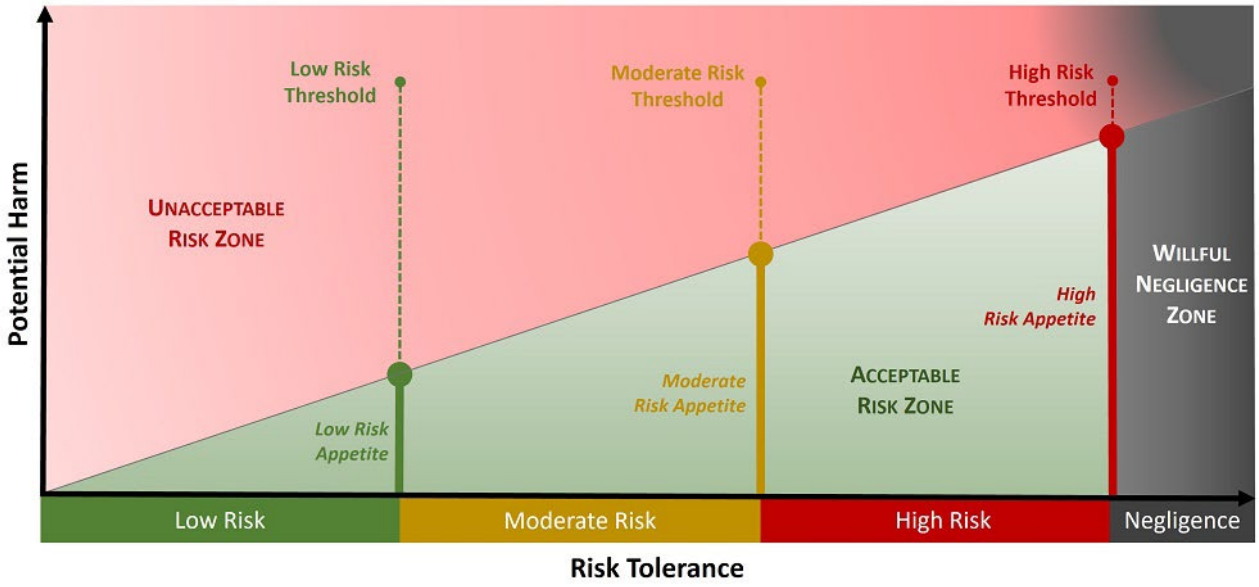
An organization's risk tolerance is influenced by several factors that includes, but are not limited to:

- Statutory, regulatory and contractual compliance obligations (including adherence to privacy principles for ethical data protection practices);
- Organization-specific threats (natural and manmade);
- Reasonably-expected industry practices;
- Pressure from competition; and
- Executive management decisions.

As it pertains to the SCF CAP, risk tolerance is simplified as being one (1) of the following three (3) levels:

- Low;
- Moderate; or
- High.

[8] *Materiality Tracker - https://www.materialitytracker.net/standards/definitions/*
[9] *Project Management Body of Knowledge (**PMBOK**) - https://www.pmi.org/pmbok-guide-standards/foundational/PMBOK*



Low Organizational Risk Tolerance

Organizations that would be reasonably-expected to adopt a low risk tolerance generally:

- Provide products and/or services that are necessary for the population to maintain normalcy in daily life;
- Are in highly-regulated industries with explicit cybersecurity and/or data protection requirements;
- Store, process and/or transmit highly-sensitive/regulated data;
- Are legitimate targets for nation-state actors to disrupt and/or compromise due to the high-value nature of the organization;
- Have strong executive management support for cybersecurity & data privacy practices as part of "business as usual" activities;
- Maintain a high level of capability maturity for preventative cybersecurity controls to implement "defense in depth" protections across the enterprise;
- Have a high level of situational awareness (cybersecurity & physical) that includes its supply chain; and
- Have cyber-related insurance.

Organizations that are reasonably-expected to operate with a low risk tolerance include, but are not limited to:

- Critical infrastructure;
- Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.);
- Telecommunications (e.g., Internet Service Providers (**ISPs**), mobile phone carriers, Cloud Service Providers (**CSPs**), etc.) (high value);
- Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.);
- Technology Research & Development (**R&D**) (high value);
- Healthcare (high value); and
- Government institutions:
  - Military;
  - Law enforcement;
  - Judicial system;
  - Financial services (high value); and
  - Defense Industrial Base (**DIB**) contractors (high value).

Moderate Organizational Risk Tolerance

Organizations that would be reasonably-expected to adopt a moderate risk tolerance generally:

- Have executive management support for securing sensitive / regulated data enclaves;
- Are in regulated industries that have specific cybersecurity and/or data protection requirements (e.g., CMMC, PCI DSS, SOX, GLBA, RMF, etc.);
- Have "flow down" requirements from customers that require adherence to certain cybersecurity and/or data protection requirements;
- Store, process and/or transmit sensitive/regulated data;
- Are legitimate targets for attackers who wish to financially benefit from stolen information or ransom; and
- Have cyber-related insurance.

Organizations that are reasonably expected to operate with a moderate risk tolerance include, but are not limited to:

- Education (e.g., K-12, colleges, universities, etc.);
- Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.);
- Telecommunications (e.g., Internet Service Providers (**ISPs**), mobile phone carriers, etc.);
- Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.);
- Technology services (e.g., Managed Service Providers (**MSPs**), Managed Security Service Providers (**MSSP**), etc.);
- Manufacturing (high value);
- Healthcare;
- Defense Industrial Base (**DIB**) contractors and subcontractors;
- Legal services (e.g., law firms); and
- Construction (high value).

High Organizational Risk Tolerance

Organizations that would be reasonably-expected to adopt a high risk tolerance generally:

- Are in an unregulated industry, pertaining to cybersecurity and/or data protection requirements;
- Do not store, process and/or transmit sensitive/regulated data;
- Lack management support for cybersecurity & data privacy governance practices; and
- Do not have cyber-related insurance.

Organizations that may choose to operate with a high risk tolerance include, but are not limited to:

- Restaurants;
- Hospitality industry;
- Construction;
- Manufacturing; and
- Personal services.

OBJECTIVITY

The SCF CAP's objective analysis is designed to put aside any potential bias by the assessor that would be inconsistent with the perspective of a reasonable stakeholder. For example, a ROC designation of a "Significant Deficiency" or "Material Weakness" may result in reputational harm, such as a decrease in the Organization Seeking Certification's (**OSC's**) share price, increased scrutiny by both investors and regulators, possible litigation or other impacts due to negative assessment results. An assessment where an assessor's biases, based on such potential impacts, influences a determination that one or more deficient controls are not material to the organization's cybersecurity & data privacy program would not be objective and would be inconsistent with the concept of materiality.

This desire to maintain objectivity is a driving factor in requiring automation in the assessment process using SCF Connect as a tool to calculate materiality decisions objectively. This is designed to ensure the ROC accurately reflects an objective evaluation of an organization's cybersecurity & data privacy practices at a single point in time.

CONFORMITY ASSESSMENT DESIGNATIONS

The CAP is designed to produce a deliverable Report on Conformity (**ROC**) with a designation that summarizes the organization's overall cybersecurity & data privacy program. Those three (3) possible designations are:

Conforms

CONFORMS

A ROC designation of "Conforms" is a positive outcome due to deficiencies not being material to the OSC's cybersecurity and/or privacy program.

This indicates that at a high-level, the organization's cybersecurity & data privacy practices conform to its selected cybersecurity & data privacy practices. At the control level, there may be one or more deficient controls, but as a whole, the cybersecurity & data privacy practices support the organization's stated risk tolerance

It is a statement that the assessed controls conform indicates to the organization's management that sufficient evidence of due care and due diligence exists to assure that the organization's stated risk tolerance can be achieved.

Significant Deficiency

SIGNIFICANT DEFICIENCY

A ROC designation of "Significant Deficiency" is a negative outcome due to the deficiencies being material to the OSC's cybersecurity and/or privacy program.

This is a negative outcome and indicates the organization was unable to demonstrate conformity with its selected cybersecurity & data privacy practices, due to systematic problems. Further, this indicates cybersecurity & data privacy practices fail to support the organization's stated risk tolerance. This is less severe than a material weakness, but merits executive leadership attention.

It is a statement that the assessed controls have a significant deficiency indicates to the organization's management that insufficient evidence of due care and due diligence exists to assure that the organization's stated risk tolerance is achieved, due to a systemic problem in the cybersecurity and/or privacy program.

In the context of a significant deficiency, a systemic problem is a consequence of issues inherent in the overall function (e.g., team, department, project, application, service, vendor, etc.), rather than a specific, isolated factor. Systemic errors may require changing the structure, personnel, technology and/or practices to remediate the significant deficiency.

Material Weakness

MATERIAL WEAKNESS

A ROC designation of "Material Weakness" is a negative outcome due to the deficiencies being material to the OSC's cybersecurity and/or privacy program.

This indicates the organization is unable to demonstrate conformity with its selected cybersecurity & data privacy practices, due to deficiencies that make it probable that reasonable-expected threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance. This indicates cybersecurity & data privacy practices fail to support the organization's stated risk tolerance.

It is statement that the assessed controls have a material weakness indicates to the organization's management that (1) the cybersecurity and/or privacy program is incapable of successfully performing its stated mission and (2) drastic changes to people, processes and/or technology are necessary to remediate the findings.

TRANSLATING RISK TOLERANCE TO SCF CAP ASSESSMENT RIGOR

There are three (3) levels of rigor that an OSC can select for its assessment:

1. Basic (Low Assurance) – this corresponds to "high risk tolerance"
2. Focused (Moderate Assurance) – this corresponds to "moderate risk tolerance"
3. Comprehensive (High Assurance) – this corresponds to "low risk tolerance"

Information Assurance (**IA**) is the practice of assuring information and managing risks related to the use, processing, storage and transmission of information or data and the systems and processes used for those purposes.

- The definition of each assessment method includes types of objects to which the method can be applied. The application of each method is described in terms of depth and coverage attributes. The attribute values correlate to the assurance requirements specified by the organization by the level of assessment rigor;
- The depth attribute addresses the rigor and level of detail of the assessment. For the depth attribute, the focused attribute value includes and builds upon the assessment rigor and level of detail defined for the fundamental attribute value; the total attribute value includes and builds upon the assessment rigor and level of detail defined for the focused attribute value; and
- The coverage attribute addresses the scope or breadth of the assessment. For the coverage attribute, the focused attribute value includes and builds upon the number and type of assessment objects defined for the fundamental attribute value; the total attribute value includes and builds upon the number and type of assessment objects defined for the focused attribute value.

Appendix A: Assessment Rigor contains a detailed breakdown of the assessment methods, based on the selected level of rigor.

100% of the Assessment Objectives (**AOs**) must be satisfied for a control to be categorized as Satisfactory as follows. All AOs must be:

- Satisfactory;
- Not Applicable (N/A); or
- A compensating control exists).

CRITERIA	Low Assurance (high risk)	Moderate Assurance (moderate risk)	High Assurance (low risk)
Conforms	▪ ≥ 80% of controls with a **weighting of ≥ 7** must have at least Maturity Level (ML) 2 that are (1) Satisfied, (2) N/A or (3) have a valid compensating control. ▪ Controls with a weighting of ≤ 6 are not required to be met. ▪ Within the same domain, ≤ 10% of controls are deficient.	▪ ≥ 80% of controls with a **weighting of ≥ 5** must have at least Maturity Level (ML) 2 that are (1) Satisfied, (2) N/A or (3) have a valid compensating control. ▪ Controls with a weighting of ≤ 4 are not required to be met. ▪ Within the same domain, ≤ 10% of controls are deficient.	▪ ≥ 80% of controls with a **weighting of ≥ 3** must have at least Maturity Level (ML) 2 that are (1) Satisfied, (2) N/A or (3) have a valid compensating control. ▪ Controls with a weighting of ≤ 2 are not required to be met. ▪ Within the same domain, ≤ 10% of controls are deficient.
Significant Deficiency	▪ 70 ≤ 80% of controls with a **weighting of ≥ 7** must have at least Maturity Level (ML) 2 that are (1) Satisfied, (2) N/A or (3) have a valid compensating control. ▪ Controls with a weighting of ≤ 6 are not required to be met. ▪ ≤ 30% of controls are deficient. ▪ Within the same domain, 10 ≤ 20% of controls are deficient.	▪ 70 ≤ 80% of controls with a **weighting of ≥ 5** must have at least Maturity Level (ML) 2 that are (1) Satisfied, (2) N/A or (3) have a valid compensating control. ▪ Controls with a weighting of ≤ 4 are not required to be met. ▪ ≤ 30% of controls are deficient. ▪ Within the same domain, 10 ≤ 20% of controls are deficient.	▪ 70 ≤ 80% of controls with a **weighting of ≥ 3** must have at least Maturity Level (ML) 2 that are (1) Satisfied, (2) N/A or (3) have a valid compensating control. ▪ Controls with a weighting of ≤ 2 are not required to be met. ▪ ≤ 30% of controls are deficient. ▪ Within the same domain, 10 ≤ 20% of controls are deficient.
Material Weakness	▪ Any control with a weighting of 10 is deficient. ▪ ≤ 70% of controls with a **weighting of ≥ 7** must have at least Maturity Level (ML) 2 that are (1) Satisfied, (2) N/A or (3) have a valid compensating control. ▪ Controls with a weighting of ≤ 6 are not required to be met. ▪ > 30% of controls are deficient. ▪ Within the same domain, > 20% of controls are deficient.	▪ Any control with a weighting of 10 is deficient. ▪ ≤ 70% of controls with a **weighting of ≥ 5** must have at least Maturity Level (ML) 2 that are (1) Satisfied, (2) N/A or (3) have a valid compensating control. ▪ Controls with a weighting of ≤ 4 are not required to be met. ▪ > 30% of controls are deficient. ▪ Within the same domain, > 20% of controls are deficient.	▪ Any control with a weighting of 10 is deficient. ▪ ≤ 70% of controls with a **weighting of ≥ 3** must have at least Maturity Level (ML) 2 that are (1) Satisfied, (2) N/A or (3) have a valid compensating control. ▪ Controls with a weighting of ≤ 2 are not required to be met. ▪ > 30% of controls are deficient. ▪ Within the same domain, > 20% of controls are deficient.

SCF CAP Level 1: Basic (Low Assurance)

A SCF CAP Level 1 "low assurance" assessment means the Organization Seeking Certification (**OSC**) has a higher risk of non-conformity. This level of assurance provides a basic level of understanding of the security measures necessary to determine whether those safeguards are:

1. Implemented according to industry-recognized secure practices; and
2. Free of obvious / apparent errors.

For a SCF CAP Level 1: Basic (Low Assurance) Assessment:

- Sensitive / regulated data types that are expressly prohibited include:
  - Sensitive Personally Identifiable Information (**sPII**) (as dictated by a law or regulation);
  - Electronic Protected Health Information (**ePHI**);
  - Cardholder Data (**CHD**) (as defined by the Payment Card Industry Security Standards Council);
  - Controlled Unclassified Information (**CUI**);

  - Commerce Control List (**CCL**) (e.g., export-controlled data that is ITAR / EAR regulated);
  - Protected Health Information (**PHI**);
  - Student Educational Records (e.g., FERPA regulated); and
  - Critical Infrastructure Information (**CII**).
- Acceptable sensitive / regulated data types include:
  - Personally Identifiable Information (**PII**) that is not covered by a law or regulation;
  - Intellectual Property (**IP**);
  - Attorney-Client Privilege Information (**ACPI**); and
  - Federal Contract Information (**FCI**).

Conforms Criteria

For CAP Level 1, a passing result of Conforms exists when:

- The OSC does not store, process and/or transmit sensitive and/or regulated data (e.g., sPII, ePHI, CUI, CHD, etc.);*
- The maturity of assessed Minimum Security Requirements (MSR) (e.g., control set) must be at least Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) Level 2 (Planned & Tracked);[10]
- At least 80% of MSR must conform:
  - Controls with a Control Weighting (CW) of 10:
    - Must be Satisfied; and
    - Cannot be:
      - Not Applicable (N/A); or
      - Compensating Control.
  - Controls with a CW of 7, 8 and 9 must be:
    - Satisfied;
    - N/A; or
    - Have a legitimate Compensating Control; and
- No more than 10% of controls within the same domain can be deficient.

If that criteria is not me, then the organization has an unsatisfactory finding:

- Significant Deficiency; or
- Material Weakness.

* By design, the SCF CAP precludes an OSC that stores, processes and/or transmits sensitive and/or regulated data from obtaining a "low assurance" SCF Certification. Any OSC that store, process and/or transmit sensitive and/or regulated data is restricted to either a Moderate or High assurance assessment. The exception to this rule is for Federal Contract Information (**FCI**), due to FCI's "low-value" as regulated data categorization. In cases where an OSC stores, processes and/or transmits FCI, the OSC may select a SCF CAP Level 1: Basic (Low Assurance) assessment.

Significant Deficiency Criteria

For CAP Level 1, an unsatisfactory finding of Significant Deficiency means:

- Between 70% and 79.9% of controls with a CW of 7, 8 and 9 are:
  - Satisfied;
  - N/A; or
  - Have a legitimate Compensating Control; and/or
- Within the same domain, between 10.1% and 20% controls are deficient.

Material Weakness Criteria

For CAP Level 1, an unsatisfactory finding of Material Weakness means:

- Controls with a CW of 10 are not satisfied;
- Less than 70% controls with a CW of 7, 8 and 9 are:
  - Satisfied;
  - N/A; or
  - Have a legitimate Compensating Control; and/or
- Within the same domain, between > 20% controls are deficient.

[10] C|P-RMM - https://securecontrolsframework.com/capability-maturity-model/

SCF CAP Level 2: Focused (Moderate Assurance)

A SCF CAP Level 2 "moderate assurance" assessment means that the OSC has a moderate risk of non-conformity. This level of assurance provides a reasonable level of understanding of the security measures necessary to determine whether those safeguards are:

1. Implemented according to industry-recognized secure practices; and
2. Operating as intended.

Conforms Criteria

For CAP Level 2, a passing result of Conforms exists when:

- The maturity of assessed MSR must be at least C|P-CMM Level 2 (Planned & Tracked);
- At least 80% of MSR must conform:
  - Controls with a Control Weighting (CW) of 10:
    - Must be Satisfied; and
    - Cannot be:
      - Not Applicable (N/A); or
      - Compensating Control.
  - Controls with a CW of 5, 6, 7, 8 and 9 must be:
    - Satisfied;
    - N/A; or
    - Have a legitimate Compensating Control; and
- No more than 10% of controls within the same domain can be deficient.

If that criteria is not me, then the organization has an unsatisfactory finding:

- Significant Deficiency; or
- Material Weakness.

Significant Deficiency Criteria

For CAP Level 1, an unsatisfactory finding of Significant Deficiency means:

- Between 70% and 79.9% of controls with a CW of 5, 6, 7, 8 and 9 are:
  - Satisfied;
  - N/A; or
  - Have a legitimate Compensating Control; and/or
- Within the same domain, between 10.1% and 20% controls are deficient.

Material Weakness Criteria

For CAP Level 2, an unsatisfactory finding of Material Weakness means:

- Controls with a CW of 10 are not satisfied;
- Less than 70% controls with a CW of 5, 6, 7, 8 and 9 are:
  - Satisfied;
  - N/A; or
  - Have a legitimate Compensating Control; and/or
- Within the same domain, between > 20% controls are deficient.

SCF CAP Level 3: Comprehensive (High Assurance)

A SCF CAP Level 3 "high assurance" assessment means the OSC has a low risk of non-conformity. This level of assurance provides a comprehensive level of understanding of the security measures necessary to determine whether those safeguards are:

1. Implemented according to industry-recognized secure practices;
2. Operating as intended on an ongoing and consistent basis; and
3. Supported continuous improvement in the effectiveness of the safeguards.

Conforms Criteria

For CAP Level 3, a passing result of Conforms exists when:

- The maturity of assessed MSR must be at least C|P-CMM Level 2 (Planned & Tracked);
- At least 80% of MSR must conform:
  - Controls with a Control Weighting (CW) of 10:
    - Must be Satisfied; and

        - Cannot be:
            - Not Applicable (N/A); or
            - Compensating Control.
    - Controls with a CW of 3, 4, 5, 6, 7, 8 and 9 must be:
        - Satisfied;
        - N/A; or
        - Have a legitimate Compensating Control; and
- No more than 10% of controls within the same domain can be deficient.

If that criteria is not me, then the organization has an unsatisfactory finding:

- Significant Deficiency; or
- Material Weakness.

Significant Deficiency Criteria

For CAP Level 3, an unsatisfactory finding of Significant Deficiency means:

- Between 70% and 79.9% of controls with a CW of 3, 4, 5, 6, 7, 8 and 9 are:
    - Satisfied;
    - N/A; or
    - Have a legitimate Compensating Control; and/or
- Within the same domain, between 10.1% and 20% controls are deficient.

Material Weakness Criteria

For CAP Level 3, an unsatisfactory finding of Material Weakness means:

- Controls with a CW of 10 are not satisfied;
- Less than 70% controls with a CW of 3, 4, 5, 6, 7, 8 and 9 are:
    - Satisfied;
    - N/A; or
    - Have a legitimate Compensating Control; and/or
- Within the same domain, between > 20% controls are deficient.

SCF CAP Structure

The SCF Council and SCF-AB designed the SCF CAP to align with industry-recognized practices for performing conformity assessments. 3PAOs and SCF Assessors are expected to be familiar with the terminology and practices covered in NIST Special Publication 2000-01, *ABC's of Conformity Assessment*:[11]

To avoid "re-inventing the wheel," the SCF CAP leverages the NIST Risk Management Framework (**RMF**) to define the lifecycle of cybersecurity & data privacy controls.[12] The RMF consists of six (6) unique phases and the CAP will cover the lifecycle of controls management to:

1) Categorize systems.
2) Select cybersecurity & data privacy controls.
3) Implement cybersecurity & data privacy controls.
4) Assess cybersecurity & data privacy controls.
5) Authorize systems, applications & services.
6) Monitor cybersecurity & data privacy controls.

In the context of the RMF, SCF Assessors shall evaluate:

- How systems/processes/services are categorized;
- The cybersecurity & data privacy controls that were selected;
- How the cybersecurity & data privacy controls were implemented;
- The method that cybersecurity & data privacy by design principles were assessed, prior to systems/services/applications going into production; and
- The ongoing monitoring of cybersecurity & data privacy controls for effectiveness.

Note: Controls with a weighting of 10 are not eligible for compensating controls in the SCF CAP.

The SCF assigns a value on a scale from 1-10, with 1 being the least important and 10 being the most important. These values are subjective, based on SCF contributor discussion, since control weighting is important to help prioritize controls and assist with the understanding what really matters from a risk management perspective. For an insight into the thought process, a control weighting of 10 was framed as "Would you do business with an organization that did not have this control in place?" where certain controls were identified as an absolute minimum from a risk threshold perspective from a "reasonable person" perspective. Those controls were designated a score of 10. On the opposite site of the spectrum, a score of 1 was deemed "nice to have" but did not materially affect risk.

Conformity Assessment Practices

To align with industry-recognized practices for conformity assessments, the SCF CAP is designed to align with the following practices:

- The SCF-AB, as the Accreditation Body, will align with[13] the following practices:
  - ISO/IEC 17011. This specifies requirements for the competence, consistent operation and impartiality of accreditation bodies assessing and accrediting conformity assessment bodies; and
  - ISO/IEC 17029. This contains general principles and requirements for the competence, consistent operation and impartiality of bodies performing validation/verification as conformity assessment activities.
- The Third-Party Assessment Organization (**3PAO**), as a Certifying Body, will align with the following practices:
  - ISO/IEC 17020. This specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities;
  - ISO/IEC 17021-1. This addresses certification of bodies performing conformity assessments; and
  - ISO/IEC 17065. This specifies requirements for bodies certifying products, processes and services.
- The OSC is expected to[14] manage Third-Party Service Providers (**TSP**) according to:
  - ISO/IEC 17050-1. This specifies general requirements for a supplier's declaration of conformity in cases where it is desirable, or necessary, that conformity of an object to the specified requirements be attested, irrespective of the sector involved; and

[11] *NIST SO 2000-01 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.2000-01.pdf*
[12] *NIST Risk Management Framework (RMF) - https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview*
[13] *The stated term "align with" does not mandate certification with ISO, just the adoption of pertinent practices.*
[14] *The stated term "expected to" does not mandate a formal requirement and reflects "reasonably expected" Cybersecurity Supply Chain Risk Management (C-SCRM) practices.*

- ISO/IEC 17050-2. This specifies general requirements for supporting documentation to substantiate a supplier's declaration of conformity, as described in ISO/IEC 17050-1.

Compensating Cybersecurity & Data Privacy Controls

In the context of the SCF CAP, a "compensating control" is defined as:

> *"Security and/or privacy controls implemented in lieu of a SCF control described in the Minimum Security Requirements (MSR) that provide equivalent or comparable protection for a system, application, service or organization. This includes management, operational and/or technical controls (e.g., safeguards or countermeasures) employed by an organization in lieu of the deficient control that reduces risk to the system, service, application, service or organization to what would be equivalent or comparable protection if the deficient control was operational and effective."*

If an OSC declares a control cannot be satisfied, it must:

1. Document the business and/or technical reason for the deficiency;
2. Identify one (1) or more other SCF controls that are specified as the designated compensating control(s); and
3. Document a description of how the compensating control(s) provides equivalent or comparable protection for the system, application, service or organization.

As part of a SCF Assessment, the SCF Assessor must validate the efficacy of the compensating control(s) through comparable assessment rigor of the other applicable SCF controls that constitute the Minimum Security Requirements (**MSR**) of the SCF Assessment.

SCF Certification Process

- SCF Certifications will be valid for two (2) year from the date of the Report on Conformity (**ROC**):
  - A template for the general layout and components of the SCF ROC will be provided to 3PAO as a means to ensure consistency among assessments and reporting; and
  - OSCs that successfully demonstrate conformance and are granted SCF Certification will be able to display the SCF Certified™ trustmark. The SCF-AB will generate the SCF Trustmark and provide it to the OSC; and
- The Third-Party Assessment, Attestation & Certification (**3PAAC**) Services will be conducted via a legally-binding contract between a 3PAO and the OSC:
  - The format and content of the Master Services Agreement (**MSA**) and Statement of Work (**SOW**) used by the 3PAO are at the discretion and responsibility of the 3PAO; and
  - The 3PAO negotiates the assessment fee structure directly with each OSC.

The SCF CAP is designed to be a two-phase approach to assessing internal controls for the assessed organization:

Phase 1 – First Party Declaration (1PD)

A First Party Declaration (**1PD**) is an annual requirement by the OSC.

- OSC performs a self-assessment that includes:
  - Scoping the environment to be assessed;
  - Identifying the appropriate controls;
  - Determining the acceptable level of conformity for the OSC (e.g., low, moderate or high assurance);
  - Gathering evidence / artifacts to demonstrate applicable evidence of due diligence and due care; and
  - Self-assessment of the evidence to determine if the OSC meets the criteria to make a 1PD;
- The organization's executive within the OSC approves the 1PD findings;
- Once the OSC has a passing declaration, the OSC identifies and contracts directly with an independent SCF Assessor to conduct 3PAAC services; and
- Upon earning a SCF Certified™ designation, the OSC has two (2) years until its next 3PAAC engagement, but it must perform an annual 1PD between 3PAAC engagements. A failing 1PD in between an OSC's bi-annual (every two (2) years) 3PAAC engagements will result in the loss of the SCF Certified™ designation.

OSCs can locate SCF-AB accredited 3PAOs on the SCF-AB's website. Prior to working with a 3PAO, the OSC is required to perform its own 1PD. Assuming the OSC has appropriate evidence to support its 1PD, it is eligible to engage with a 3PAO for a third-party assessment. This is designed to manage expectations, so that an OSC goes into a 3PAAC engagement with a solid understanding of its control strength and available evidence to support its 1PD claims.

For an OSC's Third-Party Service Providers (**TSP**):

- The OSC will be expected to provide a written Supplier Declaration of Conformity (**SDoC**) for each TSP, where the TSP declares that applicable requirements have been met based on testing, inspection or audits undertaken by the TSP or other parties on its behalf. A SDoC is generally used when:
  - The consequences (accounting for risk) associated with nonconformity are low; and
  - There are suitable penalties for non-conformity (e.g., civil tort liabilities); and
- ISO/IEC 17050-113 and ISO/IEC 17050-214 define the requirements for suppliers to meet when a formal claim that a product, service, system or persons conform to specified requirements:
  - Part 1 specifies the general requirements for an SDoC; and
  - Part 2 contains requirements for supporting documentation to substantiate the SDoC, such as reports of testing carried out by the supplier or independent third-party.

Phase 2 – Third-Party Assessment, Attestation & Certification (3PAAC)

A 3PAAC is a bi-annual (every two (2) years) requirement for OSCs to maintain the SCF Certified™ designation, where:

- The OSC engages in a legally binding contract between the OSC and its selected 3PAO;
- A SCF-accredited 3PAO performs an evaluation of the OSC's 1PD package that includes:
  - Evaluating the scope of the assessment environment to ensure it is accurate;
  - Validating the selected controls apply to the scope of the assessment;
  - Evaluating evidence / artifacts to determine if evidence of due diligence and due care exists to satisfy the selected controls;
  - Identifying a sample of controls to perform testing and
  - Testing the sample of controls to verify the controls are implemented correctly and operate properly;
- The 3PAO documents the findings of the evaluation of the OSC's 1PD package and control testing activities in a Report on Conformity (**ROC**) report that provides a passing or failing attestation from the SCF Assessor; and
- The ROC and supporting evidence is subject to Quality Control (**QC**) inspection from the SCF-AB, where ROC deficiencies would need to be finalized prior to a SCF Certified™ designation being issued to an OSC.

The SCF-AB believes in a free market approach to OSCs selecting a 3PAO. 3PAOs are expected to follow industry-recognized practices for assessment operations that include, but are not limited to:

- Billing (e.g., billable rate, method of billing, etc.);
- Assessment framing (e.g., scoping validation);
- Assessment "kick off" meetings;
- Daily outbriefs;
- Quality reviews;
- Assessment results briefing; and
- Document retention & destruction.

SCF CAP Certification Scope

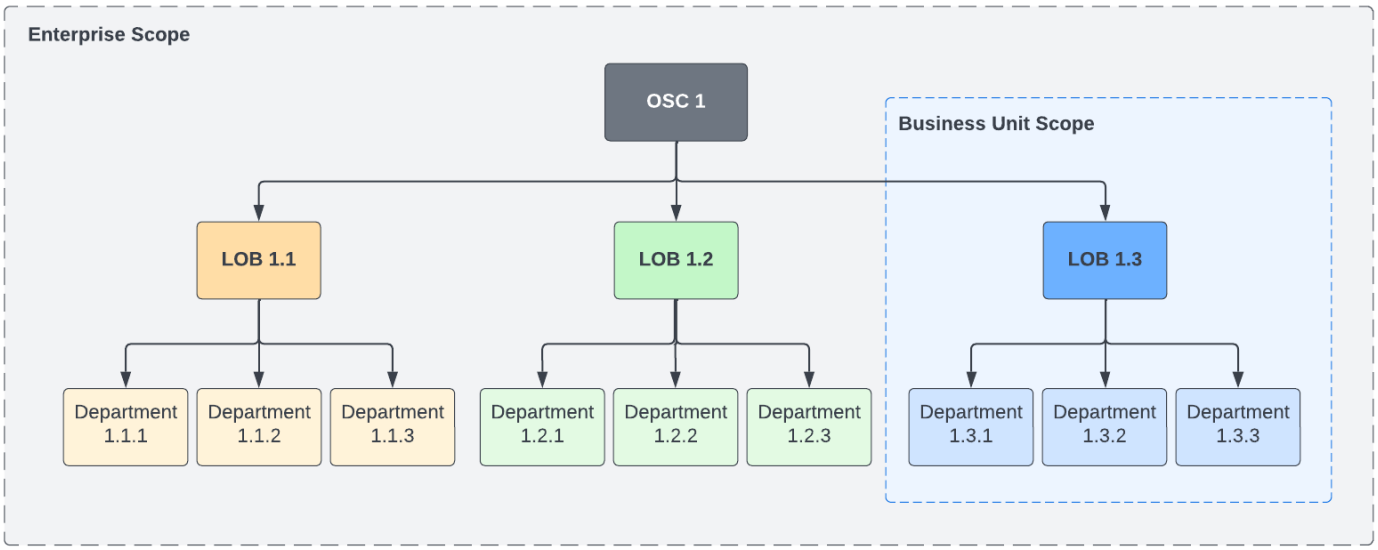
The SCF Council and SCF-AB recognize the Unified Scoping Guide (**USG**) as the authoritative source for defining in-scope vs. out-of-scope assets. Requests to deviate from the USG must be approved by the SCF-AB and it is the 3PAO's obligation to validate the approval of any deviations from the USG.

Organization vs Business Unit

The scope of a SCF CAP can be either:

1. An Organization Seeking Certification (**OSC**) in its entirety, where the legal entity is defined by a unique:
    a. Taxpayer Identification Number (**TIN**);
    b. Employer Identification Number (**EIN**);
    c. Value Added Tax (**VAT**); or
    d. Dun and Bradstreet (**D-U-N-S**); or
2. One (1) or more Business Units (**BUs**) within the OSC. This is a Line of Business (**LOB**) within an OSC that is defined by:
    a. The OSC with enough detail to:
        i. Accurately describe the LOB; and
        ii. Establish the assessment boundary; or
    b. Commercial And Government Entity (**CAGE**) Code that is applicable to a specific LOB.

This concept of scoping by the entire entity of the OSC or by a BU/LOB can be visualized in the graphic shown below:



Defining Control Applicability

The SCF CAP requires the OSC to define its Minimum Security Requirements (**MSR**), according to applicable Minimum Compliance Requirements (MCR) and Discretionary Security Requirements (**DSR**) criteria.

- The controls defined as MSR constitute the scope of the controls for the SCF CAP; and
- Applicable Assessment Objectives (**AOs**) for the MSR will be used to evaluate control implementation.

The Unified Scoping Guide (**USG**) shall be used to define the scope of the SCF CAP for an OSC and the assessment boundary.[15]

Unified Scoping Guide (USG)

The USG is a free resource that is intended to help organizations define the scope of the sensitive / regulated data where it is stored, transmitted and/or processed. This guide will refer to both sensitive and regulated data as "sensitive data" to simplify the concept for which document is focused.

This model categorizes system components according to several factors:

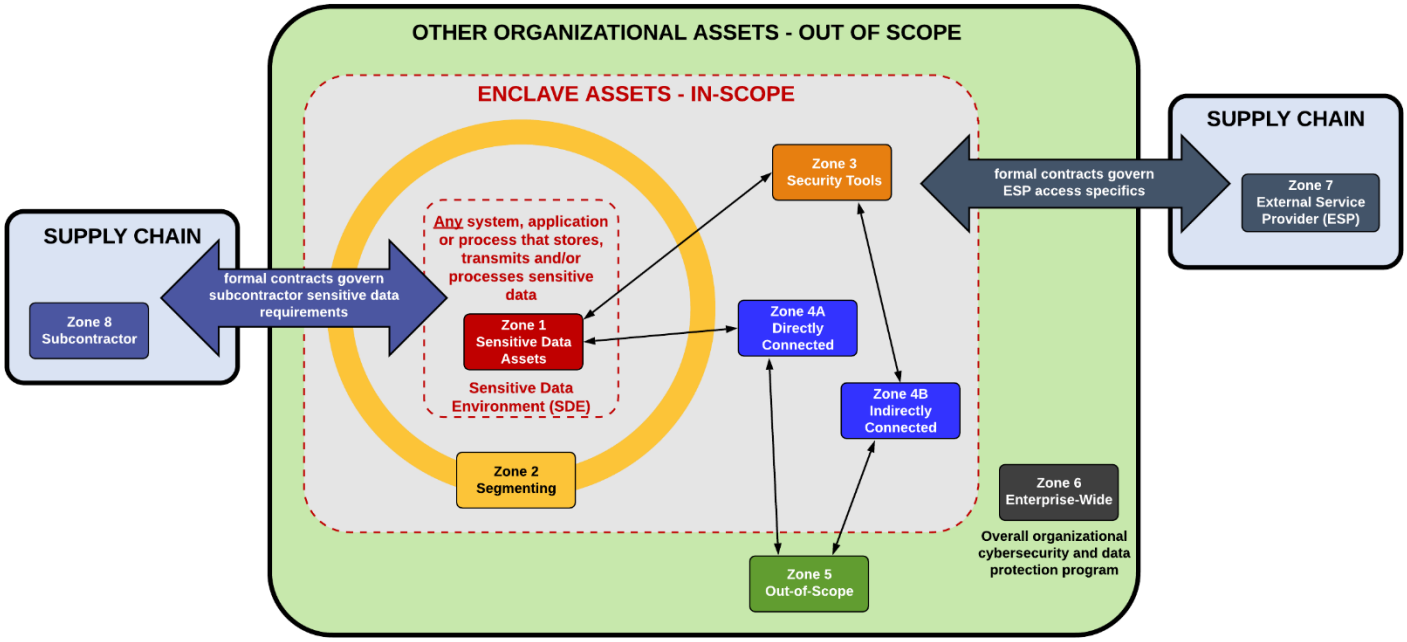
- Whether sensitive / regulated data is being stored, processed or transmitted;
- The functionality that the system component provides (e.g., access control, logging, antimalware, etc.); and

[15] *Unified Scoping Guide - https://www.unified-scoping-guide.com/sensitive-regulated-data-scoping-guide*

- The connectivity between the system and the sensitive / regulated data environment.

This approach applies to the following sensitive / regulated data types:

- Controlled Unclassified Information (**CUI**);
- Personally Identifiable Information (**PII**);
- Cardholder Data (**CHD**);
- Attorney-Client Privilege Information (**ACPI**);
- Export-Controlled Data (**ITAR / EAR**);
- Federal Contract Information (**FCI**);
- Protected Health Information (**PHI**);
- Intellectual Property (**IP**);
- Student Educational Records (**FERPA**); and
- Critical Infrastructure Information (**CII**).



When viewing scoping, there are eight (8) zones for sensitive / regulated data compliance purpose:

1. Sensitive Data Assets: Systems, services and applications that directly store, transmit and/or process sensitive /regulated data.
2. Segmenting: "Segmenting systems" that provide access (e.g., firewall, hypervisors, etc.).
3. Security Tools: "Security tools" that directly impact the integrity of category 1 and 2 assets (e.g., Active Directory, centralized antimalware, vulnerability scanners, IPS/IDS, etc.).
4. Connected. "Connected systems" that are systems, embedded technologies, applications or services that directly, or indirectly, connect to the sensitive / regulated data environment. Systems, embedded technologies, applications and services that may impact the security of (for example, name resolution or web redirection servers) the sensitive / regulated data environment are always in scope. Essentially, it something can impact the security of sensitive / regulated data, it is in scope.
5. Out-of-Scope. Out-of-scope systems that are entirely isolated from the sensitive / regulated data systems.
6. Enterprise-Wide. Addresses the organization's overall corporate security program (cyber and physical).
7. External Service Provider. Supply-chain security with the "flow down" of contractual requirements to External Service Providers (ESPs) that can directly or indirectly influence the sensitive / regulated data environment. ESPs are third-party organizations that provide services to the organizations.
8. Subcontractors. Addresses subcontractors, which are third-party organizations that are party to the actual execution of the contract where the subcontractor may create, access, receive, store and/or transmit regulated data (sensitive / regulated data).

GLOSSARY

ACRONYMS

Accreditation Body (**AB**)
Applications, Services and Processes (**ASP**)
Capability Maturity Model (**CMM**)
Certifying Body (**CB**)
Commercial-Off-The-Shelf (**COTS**)
Common Weakness Enumeration (**CWE**)
Computerized Numerical Control (**CNC**)
Confidentiality, Integrity, Availability and Safety (**CIAS**)
Cloud Service Provider (**CSP**)
Cyber-Physical Systems (**CPS**)
Cybersecurity Supply Chain Risk Management (**C-SCRM**)
Defense Acquisition Regulations System (**DFARS**)
Defense Industrial Base (**DIB**)
Development & Operations (**DevOps**)
Discretionary Security Requirements (**DSR**)
Distributed Denial of Service (**DDoS**)
Enterprise Information Technology (**EIT**)
Executive Assessment Report (**EAR**)
Executive Order (**EO**)
Federal Acquisition Regulation (**FAR**)
First Party Conformity Assessment Activity (**1PCAA**)
First Party Declaration (**1PD**)
Garbage In, Garbage Out (**GIGO**)
Governance, Risk Management and Compliance (**GRC**)
Government-Off-The-Shelf (**GOTS**)
High Value Asset (**HVA**)
High Value Target (**HVT**)
Individual Contributors (**IC**)
Industrial Control Systems (**ICS**)
Information Assurance (**IA**)
Integrated Controls Management (**ICM**)
International Organization for Standardization (**ISO**)
Internet Service Provider (**ISP**)
Master Services Agreement (**MSA**)
Minimum Compliance Requirements (MCR)
Minimum Security Requirements (**MSR**)
Minimum Viable Product (**MVP**)
National Institute of Standards and Technology (**NIST**)
Open Web Application Security Project (**OWASP**)
Operating Systems (**OS**)
Operational Technology (**OT**)
Organization Seeking Certification (**OSC**)
Programmable Logic Controllers (**PLCs**)
Report on Conformity (**ROC**)
Research & Development (**R&D**)
Risk Management Framework (**RMF**)
SCF Accreditation Body (**SCF-AB**)
SCF Assessment Objective (**AO**)
SCF Certification Requirement (**SCR**)
SCF Conformity Assessment (**SCA**)
SCF Third Party Assessment Organization (**3PAO**)
Secure Controls Framework (**SCF**)
Secure Control Framework Conformity Assessment Program (**SCF CAP**)
Secure Development Lifecycle (**SDL**)
Secure Software Development Framework (**SSDF**)
Secure Software Development Practices (**SSDP**)
Security, Development & Operations (**SecDevOps**)
Sharable Assessment Report (**SAR**)
Software Bill of Materials (**SBOM**)
Software Supply Chain Security (**SSCS**)
Software/System Development Life Cycle (**SDLC**)
Single Source of Truth (**SSOT**)
Statement of Work (**SOW**)
Supplier Declaration of Conformity (**SDoC**)
Supply Chain Risk Management (**SCRM**)
System(s) of Record (**SOR**)
Team Leader (**TL**)
Technical Assessment Report (**TAR**)
Technical Experts (**TE**)
Third-Party Assessment, Attestation & Certification (**3PAAC**)
Third-Party Assessment Organization (**3PAO**)
Third-Party Service Providers (**TSP**)
Trustworthy Secure Design (**TSD**)
Unified Scoping Guide (**USG**)

DEFINITIONS

The SCF-AB recognizes two (2) 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;[16] and
- NIST Glossary.[17]

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.[18]

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

APPENDIX A: ASSESSMENT RIGOR

The SCF CAP's assessment rigor is based on the concepts from Appendix C of NIST SP 800-172A.[19]

SCF CAP LEVEL 1: BASIC

Basic assessments provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors.

The definition of each assessment method includes types of objects to which the method can be applied. In addition, the application of each method is described in terms of the attributes of depth and coverage.

- The depth attribute addresses the rigor and level of detail of the assessment.
- The coverage attribute addresses the scope or breadth of the assessment.

BASIC Assessment Rigor		EXAMINE	INTERVIEW	TEST
Method		The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness and potential for improvement over time.	The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness and potential for improvement over time.	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness and potential for improvement over time.
Objects	Specifications	- Policies - Plans - Procedures - System requirements - Designs	N/A	N/A
	Mechanisms	- Functionality implemented in hardware, software and firmware.	N/A	- Hardware - Software - Firmware
	Activities	- System operations - Administration - Management - Exercises	N/A	- System operations - Administration - Management - Exercises
	Individuals or Groups	N/A	Examples: Personnel with risk assessment responsibilities; personnel with information security responsibilities; system or network administrators; and personnel with account management responsibilities.	N/A
Attributes	Depth	An examination that consists of high-level reviews, checks, observations or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation. Examples include: functional-level descriptions for mechanisms; high-level process descriptions for activities; and documents for specifications. Basic examinations provide a level of understanding	An interview that consists of broad-based, high-level discussions with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions. Basic interviews provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors.	A test methodology (also known as black box testing) assumes no knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification for mechanisms and a high-level process description for activities. Basic testing provides a level of understanding of the security measures necessary for determining whether the

[19] *NIST SP 800-172A - https://csrc.nist.gov/publications/detail/sp/800-172a/final*

		of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors.		safeguards are implemented and free of obvious errors.
	Coverage	An examination that uses a representative sample of assessment objects (by type and number within type) to provide the level of coverage necessary for determining whether the security measures are implemented and free of obvious errors.	An interview that uses a representative sample of individuals in organizational roles to provide the level of coverage necessary for determining whether the security measures are implemented and free of obvious errors.	Addresses the scope or breadth of the testing process and includes the types of assessment objects to be tested; the number of objects to be tested by type; and specific objects to be tested.

SCF CAP LEVEL 2: FOCUSED

Focused assessments provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious / apparent errors and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.

The definition of each assessment method includes types of objects to which the method can be applied. In addition, the application of each method is described in terms of the attributes of depth and coverage.

- The depth attribute addresses the rigor and level of detail of the assessment.
- The coverage attribute addresses the scope or breadth of the assessment.

FOCUSED Assessment Rigor		EXAMINE	INTERVIEW	TEST
Method		The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness and potential for improvement over time.	The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness and potential for improvement over time.	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness and potential for improvement over time.
Objects	Specifications	- Policies - Plans - Procedures - System requirements - Designs	N/A	N/A
	Mechanisms	- Functionality implemented in hardware, software and firmware.	N/A	- Hardware - Software - Firmware
	Activities	- System operations - Administration - Management - Exercises	N/A	- System operations - Administration - Management - Exercises
	Individuals or Groups	N/A	Examples: Personnel with risk assessment responsibilities; personnel with information security responsibilities; system or network administrators; and personnel with account management responsibilities.	N/A

Attributes	Depth	An examination that consists of high-level reviews, checks, observations or inspections and more in-depth studies and analyses of the assessment object. This type of examination is conducted using a substantial body of evidence or documentation. Examples include: functional-level descriptions and where appropriate and available, high-level design information for mechanisms; high-level process descriptions and implementation procedures for activities; and documents and related documents for specifications. Focused examinations provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.	An interview that consists of broad-based, high-level discussions and more in- depth discussions in specific areas with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in-depth questions in specific areas where responses indicate a need for more in-depth investigation. Focused interviews provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.	A test methodology (also known as gray box testing) assumes some knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification and limited system architectural information (e.g., high-level design) for mechanisms and a high-level process description and high-level description of integration into the operational environment for activities. Focused testing provides a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.
	Coverage	An examination that uses a representative sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining whether the security measures are implemented and free of obvious errors and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.	An interview that uses a representative sample of individuals in organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining whether the security measures are implemented and free of obvious errors and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.	Testing that uses a representative sample of assessment objects by type and number within type and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining whether the security measures are implemented and free of obvious errors and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.

SCF CAP LEVEL 3: COMPREHENSIVE

Comprehensive assessments provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are further increased grounds for confidence that the safeguards are implemented correctly and operating as intended on an ongoing and consistent basis and that there is support for continuous improvement in the effectiveness of the safeguards.

The definition of each assessment method includes types of objects to which the method can be applied. In addition, the application of each method is described in terms of the attributes of depth and coverage.

- The depth attribute addresses the rigor and level of detail of the assessment.
- The coverage attribute addresses the scope or breadth of the assessment.

COMPREHENSIVE Assessment Rigor		EXAMINE	INTERVIEW	TEST
Method		The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness and potential for improvement over time.	The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness and potential for improvement over time.	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness and potential for improvement over time.
Objects	Specifications	- Policies - Plans - Procedures - System requirements - Designs	N/A	N/A
	Mechanisms	- Functionality implemented in hardware, software and firmware.	N/A	- Hardware - Software - Firmware
	Activities	- System operations - Administration - Management - Exercises	N/A	- System operations - Administration - Management - Exercises
	Individuals or Groups	N/A	Examples: Personnel with risk assessment responsibilities; personnel with information security responsibilities; system or network administrators; and personnel with account management responsibilities.	N/A

Attributes	Depth	An examination that consists of high-level reviews, checks, observations or inspections and more in-depth, detailed and thorough studies and analyses of the assessment object. This type of examination is conducted using an extensive body of evidence or documentation. Examples include: functional-level descriptions and where appropriate and available, high-level design information, low-level design information and implementation information for mechanisms; high-level process descriptions and detailed implementation procedures for activities; and documents and related documents for specifications. Comprehensive examinations provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are further increased grounds for confidence that the safeguards are implemented correctly and operating as intended on an ongoing and consistent basis and that there is support for continuous improvement in the effectiveness of the safeguards.	An interview that consists of broad-based, high-level discussions and more in- depth, probing discussions in specific areas with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in-depth, probing questions in specific areas where responses indicate a need for more in-depth investigation. Comprehensive interviews provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are further increased grounds for confidence that the safeguards are implemented correctly and operating as intended on an ongoing and consistent basis and that there is support for continuous improvement in the effectiveness of the safeguards.	Test methodology (also known as white box testing) that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification, extensive system architectural information (e.g., high-level design, low-level design) and implementation representation (e.g., source code, schematics) for mechanisms and a high-level process description and detailed description of integration into the operational environment for activities. Comprehensive testing provides a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are further increased grounds for confidence that the safeguards are implemented correctly and operating as intended on an ongoing and consistent basis and that there is support for continuous improvement in the effectiveness of the safeguards.
	Coverage	An examination that uses a sufficiently large sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining whether the security measures are implemented and free of obvious errors and whether there are further increased grounds for confidence that the safeguards are implemented correctly and operating as intended on an ongoing and consistent basis and that there is support for continuous improvement in the effectiveness of the safeguards.	An interview that uses a sufficiently large sample of individuals in organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining whether the security measures are implemented and free of obvious errors and whether there are further increased grounds for confidence that the safeguards are implemented correctly and operating as intended on an ongoing and consistent basis and that there is support for continuous improvement in the effectiveness of the safeguards.	Testing that uses a sufficiently large sample of assessment objects by type and number within type and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining whether the security measures are implemented and free of obvious errors and whether there are further increased grounds for confidence that the safeguards are implemented correctly and operating as intended on an ongoing and consistent basis and that there is support for continuous improvement in the effectiveness of the safeguards.

APPENDIX B: REQUIREMENTS FOR CONFORMITY ASSESSMENT BODIES (3PAO) & SCF ASSESSORS

The SCF Council and SCF-AB recognize the financial and logistical benefits to adopting "common sense" practices for establishing baseline requirements for SCF Assessors and 3PAOs. Where applicable, industry-leading practices are leveraged to avoid unnecessary redundancy and cost.

SCF ASSESSOR CERTIFICATION REQUIREMENTS

There are four (4) components to SCF Assessor certification:

1. Demonstrating minimum professional certification requirements;
2. Paying an annual registration fee;
3. Sponsorship from one (1) or more 3PAOs; and
4. Agree to adhere to the SCF Assessor Code of Conduct.

DoD 8570-01 Certification Reciprocity

To establish minimum certification requirements for SCF Assessors, the CAP derives its requirements from the DoD-approved 8570-01 baseline certifications for the Information Assurance Technician (**IAT**) Level III and Cyber Security Service Provider (**CSSP**) Auditor roles. [20]

SCF Assessors must have at least one (1) of the following certifications:

1. Certified Information Systems Auditor (**CISA**) through Information Systems Audit and Control Association (**ISACA**);
2. Certified Information Systems Security Professional (**CISSP**) through International Information Systems Security Certifications Consortium **(ISC)2**;
3. Cisco Certified Network Professional-Security (**CCNP-Security**) through Cisco;
4. GIAC Certified Enterprise Defender (**GCED**) through Global Information Assurance Certification (**GIAC**); or
5. GIAC Systems and Network Auditor (**GSNA**) through GIAC

Annual Registration Fee

A non-refundable, annual fee for an individual to have the SCF Assessor designation is $500.00 (USD). A digital badge will be generated upon payment and validation of professional certifications that will be valid for one (1) year.

During that period of validity, the individual is authorized to perform 3PAAC services, while under the sponsorship of a Third-Party Assessment Organization (**3PAO**).

3PAO Sponsorship

An individual can sign up and pay to become a SCF Assessor without first having 3PAO sponsorship. In that period of time without active 3PAO sponsorship, the individual is designated as a Provisional SCF Assessor and is not capable of performing 3PAAC services.

A 3PAO is able to sponsor a Provisional SCF Assessor by selecting the individual through SCF Connect. The SCF Assessor's assigned certificate number will be used by the 3PAO to sponsor the SCF Assessor. Once that process is complete, the SCF Assessor is authorized to perform 3PAAC services for that specific 3PAO.

A SCF Assessor may be sponsored by more than one (1) 3PAO. This enables a SCF Assessor to be either:

- Employed by 3PAO (e.g., W-2 employee); or
- A formal contractor of the 3PAO (e.g., 1099 contractor).

3PAO ACCREDITATION

3PAO are expected to align with ISO/IEC 17020:2012, *Conformity assessment — Requirements for the operation of various types of bodies performing inspection*. While not mandatory, 3PAOs should obtain and maintain a "management system certification" which is a third-party attestation related to systems within an organization. Certification of management systems is generally used to demonstrate fulfilment of quality, security and environmental management system standards.

In addition to aligning ISO/IEC 17020_2012, 3PAOs must:

- Provide a written background on the company that documents experience in performing assessment-related services;
- Provide resumes for at least two (2) personnel who are qualified to perform **SCF Assessor** duties, where at least one (1) must be an employee of the 3PAO; and

[20] *DoD-approved 8570-01 baseline certifications - https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/*

- Pay a non-refundable application fee of $5,000. Annual 3PAO registration fee renewals will be $5,000 per year, due annually upon the anniversary of 3PAO designation.

To create impartiality that prevents 3PAO from "soft balling" reports that serve only to encourage the rehiring of the 3PAO on an ongoing basis for 3PAAC services:

- A 3PAO will only be able to assess a client for no more than four (4) consecutive years. This applies at the company level, not at the individual assessor level. This company-level rotation will encourage objective assessments by 3PAO; and
- In the "off years":
  - 3PAO it can provide consulting and other professional services to a client, but not 3PAAC services in the function of a 3PAO; and
  - In scenarios where the 3PAO provides consulting or other professional services to a client that impacts / affects the implementation of SCF controls, the 3PAO cannot perform 3PAAC services for one (1) year following the end of the consulting, or other professional services engagement.

CONFLICT OF INTEREST (COI) AVOIDANCE

To avoid any perception of Conflict of Interest (**COI**), the SCF-AB's recommendation is to avoid any 3PAAC engagements that have or allude to a COI between a 3PAO and the OSC. 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 OSC it is engaged in a contract with for 3PAAC services. The SCF-AB and SCF Council identify the minimum elapsed time necessary to avoid COI for 3PAOs and/or SCF Assessors:

- At least two (2) years from the completion date of consulting services that were non-material to the OSC's Information Security Management System (ISMS); and
- At least five (5) years from the completion date of consulting services that were material to the OSC's ISMS.

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 OSC that involved:
  - Limited to suggesting improvements to the OSC's existing policies, standards and/or procedures;
  - Recommending, architecting and/or implementing technology that indirectly impacts the ISMS (e.g., security training, O365 licensing sales, etc.);
  - Tuning a Security Incident Event Manager (SIEM); and/or
  - Not related to performing an audits / gap assessments for the OSC, where the SCF Assessor's work was part of the audit / gap assessment team.
- "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 OSC that involved:
  - Recommending, architecting, authoring and/or implementing policies, standards and/or procedures;
  - Recommending, architecting and/or implementing technology that directly impacts the ISMS (e.g., SIEM, ITAM, MFA, IAM, etc.);
  - Recommending, architecting and/or defining the scope of cybersecurity and/or privacy controls;
  - Acting as part of an audit / gap assessment team where the results of such activities were used to improve the ISMS; and/or
  - Acting as a "virtual CISO" or similar authoritative role.

APPENDIX C: UNDERSTANDING THE ROLE OF SECURITY MECHANISMS

The SCF CAP points to the Secure Code Alliance (**SCA**) Demonstrating Cybersecurity & Data Privacy in Practice (**DSPP**) initiative that focuses on the holistic concepts of how broader business planning and analysis ultimately leads to actionable cybersecurity & data privacy requirements. Understanding this hierarchical nature of requirements is a fundamental construct of cybersecurity & data privacy control governance processes.

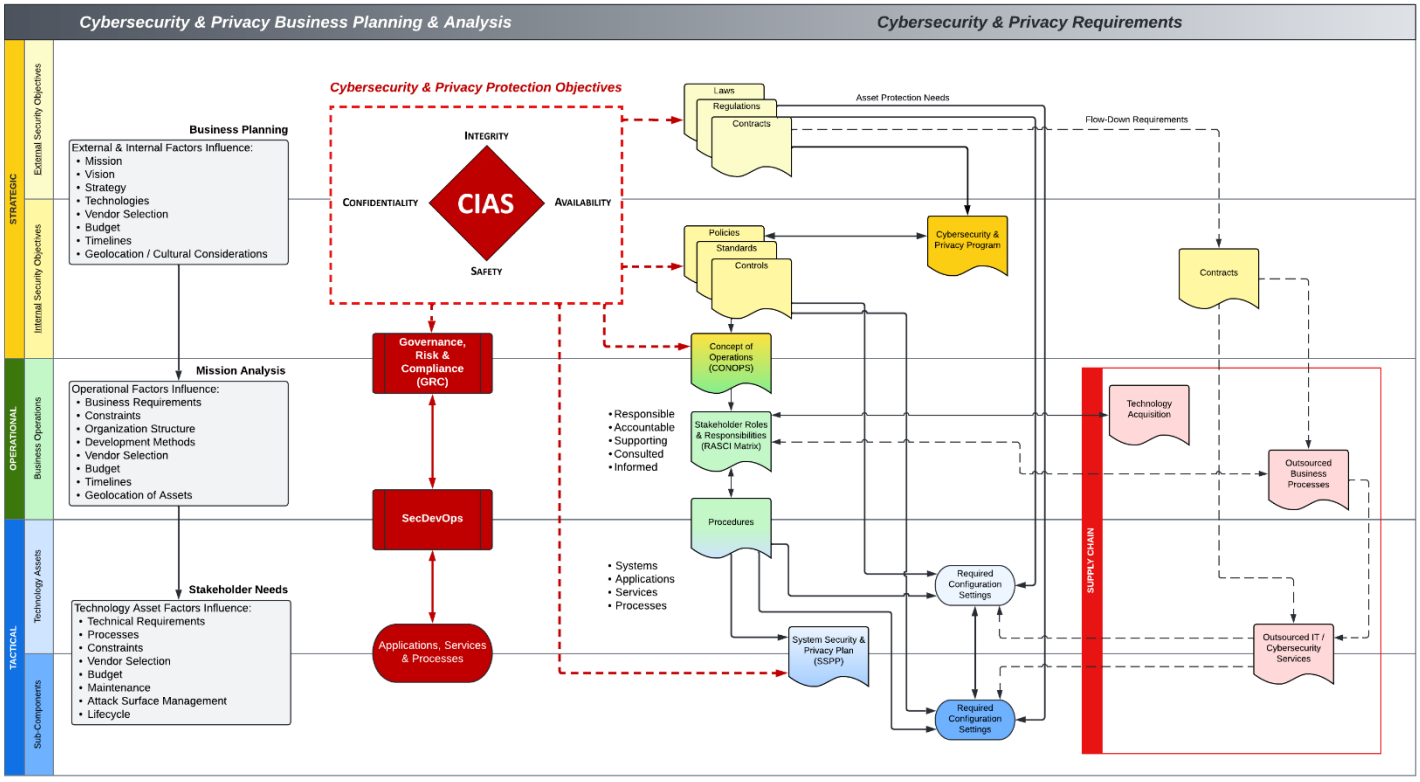
ADEQUATE SECURITY

The SCF CAP recognizes that no technology can provide absolute security due to the limits of human certainty, this uncertainty that exists in the life cycle of every system and the constraints of cost, schedule, performance, feasibility and practicality. Therefore, trade-offs are expected to be routinely made across contradictory, competing and conflicting needs and limitations. However, these trade-offs must be optimized to achieve "adequate security," reflecting a risk-based decision by stakeholders. [21]

An organization publishes policies to eliminate potential gaps in that desired governed behavior to achieve "adequate security" for the organization based on what a reasonable individual would be expected to do in a similar situation. The rules associated with this "governed behavior" must be accurate, consistent, compatible and complete with respect to the executive leadership's objectives to successfully accomplish the organization's mission and overall strategy.

An organization's policies ultimately define the behavior of Individual Contributors (**IC**) (e.g., developers) in performing their roles and associated responsibilities for developing processes and procedures. This eventually leads to the configuration of technology assets (e.g., systems, applications, services and processes), where a discrete set of restrictions and properties must exist to specify how that asset enforces, or contributes to enforcing, the organizational security policies.

This concept is depicted in the graphic shown below:[22]



The required configuration settings for technology assets must include technical and business requirements, which ultimately fall under organizational cybersecurity & data privacy policies. Requirements can be categorized as: [23]

- Stakeholder requirements that address the need to be satisfied in a design-independent manner; and
- System requirements express the specific solution that will be delivered (design-dependent manner).

[21] *NIST SP 800-160 Vol 1 Rev 1 (draft) Appendix C*
[22] *Concept to build adequate cybersecurity and privacy by design and default http://concept.securecodealliance.com*
[23] *NIST SP 800-160 Vol 1 Rev 1 (draft) Appendix C*

SECURE SYSTEMS

A "secure system" is a system that ensures that only the authorized intended behaviors and outcomes occur, thereby providing freedom from those conditions, both intentionally/with malice and unintentionally/without malice, that can cause a loss of information assets with unacceptable consequences.[24] This definition expresses an ideal that captures three (3) essential aspects of what it means to achieve security:

1. Enable the delivery of the required system capability despite intentional and unintentional forms of adversity;
2. Enforce constraints to ensure that only the desired behaviors and outcomes associated with the required system capability are realized while satisfying the first aspect; and
3. Enforce constraints based on rules to ensure that only authorized human-to-machine and machine-to-machine interactions and operations are allowed to occur while satisfying the second aspect.

For a system, adequate security is an evidence-based determination that achieves and optimizes security performance against all other performance objectives and constraints. Judgments of adequate security are driven by the stakeholder objectives, needs and concerns associated with the system. Adequate security has two elements:

- Achieve the minimum acceptable threshold of security performance; and
- Maximize security performance to the extent that any additional increase in security performance results in degrading some other aspect of system performance or requires an unacceptable operational commitment.

Stakeholder Security Requirements

Stakeholder security requirements are those stakeholder requirements that are security-relevant. Stakeholder security requirements specify:

- The protection needed for the mission or business, data, information, processes, functions, humans and system assets;
- The roles, responsibilities and security-relevant actions of individuals who perform and support the mission or business processes;
- The interactions between the security-relevant solution elements; and
- The assurance that is to be obtained in the security solution.

System Security Requirements

System requirements specify the technical view of a system or solution that meets the specified stakeholder needs. The system requirements are a transformation of the validated stakeholder requirements. System requirements specify what the system or solution must do to satisfy the stakeholder requirements. System security requirements are those system requirements that are security relevant. These requirements define:

- The protection capabilities provided by the security solution;
- The performance and behavioral characteristics exhibited by the security solution;
- Assurance processes, procedures and techniques;
- Constraints on the system and the processes, methods and tools used to realize the system; and
- The evidence required to determine the system security requirements have been satisfied.

SYSTEM OF SYSTEMS MINDSET

A system is *"an arrangement of parts or elements that together exhibit a behavior or meaning that the individual constituents do not."*[25] Since developers do not design, code and maintain Applications, Services and Processes (**ASP**) in a vacuum, developers need to embrace a "system of systems" mindset toward system interaction since there are legitimate cybersecurity & data privacy concerns with untrustworthy dependencies. A system of systems is a *"set of systems and system elements interacting to provide a unique capability that none of the constituent systems can accomplish on their own."*[26] A system of systems consists of several constituent systems plus any inter-system infrastructure, facilities and processes necessary to enable the constituent systems to integrate or interoperate.

This concept includes "interfacing systems" that have an interface for exchanging data or information, energy or other resources. Interfacing systems have two specific subsets:

- Enabling Systems. These provide essential services required to create and sustain the system. Examples of enabling systems include:
  - Software development environments;
  - Production systems;

[24] *NIST SP 800-160 Vol 1 Rev 1 (draft)*
[25] *NIST SP 800-160 Vol 1 Rev 1 (draft)*
[26] *NIST SP 800-160 Vol 1 Rev 1 (draft)*

  - Training systems; and
  - Maintenance systems; and
- Interoperating Systems. These interact with systems for the purpose of jointly performing a function during the utilization and sustainment stages of the system life cycle. Interoperating systems often form a system of systems.

APPENDIX D: SCF EVIDENCE REQUEST LIST (ERL)

The SCF-AB and SCF Council designate the Evidence Request List (**ERL**) as the official catalog of evidence for a SCF Assessment. The ERL is designed to standardize and streamline the evidence request process for a SCF Assessment to identify reasonably-expected artifacts/evidence to meet applicable SCF controls.

#	ERL #	Area of Focus	Documentation Artifact	Artifact Description	SCF Control Mappings
1	E-GOV-01	Cybersecurity & Data Protection Management	Charter - Cybersecurity Program	Documented evidence of a corporate-level (C-Level) organization and resourcing for a cybersecurity & data protection governance program.	GOV-01
2	E-GOV-02	Cybersecurity & Data Protection Management	Charter - Privacy Program	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of privacy management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01 PRI-01
3	E-GOV-03	Cybersecurity & Data Protection Management	Charter - Cybersecurity Steering Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of cybersecurity management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.1 GOV-01.2
4	E-GOV-04	Cybersecurity & Data Protection Management	Charter - Privacy Steering Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of privacy management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.2 CPL-02
5	E-GOV-05	Cybersecurity & Data Protection Management	Charter - Audit Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of internal and external audit management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.2 CPL-02
6	E-GOV-06	Cybersecurity & Data Protection Management	Charter - Risk Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of risk management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.2 CPL-02
7	E-GOV-07	Cybersecurity & Data Protection Management	Charter - Data Management Board (DMB)	Documented evidence of the organization's Data Management Board (DMB) charter and mission.	GOV-01.2
8	E-GOV-08	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Policies	Documented evidence of an appropriately-scoped cybersecurity & data protection policies. Policies are high-level statements of management intent from an organization’s executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes. Policies are enforced by standards and further implemented by procedures to establish actionable and accountable requirements.	GOV-02 PRI-01
9	E-GOV-09	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Standards	Documented evidence of an appropriately-scoped cybersecurity & data protection standards. Standards are mandatory requirements regarding processes, actions and configurations. Standards are intended to be granular and prescriptive to ensure systems, applications and processes are designed and operated to include appropriate cybersecurity & data protection protections	GOV-02

10	E-GOV-10	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Controls	Documented evidence of an appropriately-scoped cybersecurity & data protection controls. Controls are technical, administrative or physical safeguards. Controls are the nexus used to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes. Controls directly map to standards, since control testing is designed to measure specific aspects of how standards are actually implemented.	GOV-09 CPL-01 CPL-01.2
11	E-GOV-11	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Procedures	Documented evidence of an appropriate appropriately-scoped cybersecurity & data protection procedures. Procedures are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard. Procedures help address the question of how the organization actually operationalizes a policy, standard or control. The result of a procedure is intended to satisfy a specific control. Procedures are also commonly referred to as “control activities.”	GOV-02 OPS-01.1
12	E-GOV-12	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Policies & Standards Reviews	Documented evidence of a periodic review process for the organization's cybersecurity & data protection policies and standards to identify necessary updates.	GOV-03
13	E-GOV-13	Cybersecurity & Data Protection Management	Measures of Performance (Metrics)	Documented evidence of formal measure of performance that are used to track the health of the cybersecurity & data protection program (e.g., metrics, KPIs, KRIs).	GOV-01.2 GOV-05 CPL-02
14	E-AST-01	Asset Management	IT Asset Management (ITAM)	Documented evidence of an IT Asset Management (ITAM) program.	AST-01 AST-03 AST-03.1 AST-10
15	E-AST-02	Asset Management	Asset Scoping Guidance	Documented evidence of an asset scoping guidance. This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on defining in-scope systems, applications, services, processes and third-parties.	AST-04.1 AST-04.2 AST-04.3 CPL-01.2 IAO-01.1
16	E-AST-03	Asset Management	Asset Disposal Evidence	Documented evidence of a Vulnerability & Patch Management Program (VPMP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	AST-09 DCH-08 DCH-09 DCH-09.1
17	E-AST-04	Asset Management	Asset Inventories - Hardware	Documented evidence of an inventory of the organization's technology hardware assets.	AST-02
18	E-AST-05	Asset Management	Asset Inventories - Software	Documented evidence of an inventory of the organization's software assets.	AST-02
19	E-AST-06	Asset Management	Asset Inventories - Cloud Service Provider (CSP)	Documented evidence of an inventory of the organization's cloud-based services (e.g., SaaS, IaaS, PaaS, etc.).	CLD-01 CLD-09 TPM-01.1
20	E-AST-07	Asset Management	Cyber-Physical Systems (CPS)	Documented evidence of an inventory of the organization's physical assets that process functions based on software and networks.	AST-02 EMB-01
21	E-AST-08	Asset Management	Asset Inventories - Sensitive / Regulated Data	Documented evidence of an inventory of the organization's sensitive/regulated data (including systems where sensitive/regulated data is stored, processed and/or transmitted).	CLD-10 DCH-06.2 BCD-11.2 PRI-05.5

22	E-AST-09	Asset Management	Computer Lifecycle Plan (CLP)	Documented evidence of a Computer Lifecycle Plan (CLP) that describes how the life of technology assets is managed.	SEA-07.1 TDA-17
23	E-AST-10	Asset Management	Prohibited Equipment List (PEM)	Documented evidence of equipment identified by Federal Acquisition Regulation (FAR) section 889 prohibitions for certain telecommunications equipment.	AST-17
24	E-AST-11	Asset Management	Data Retention Program	Documented evidence of a formal data retention program that governs the retention and destruction of data types.	DCH-18 MON-10 PRI-05
25	E-AST-12	Asset Management	Secure Baseline Configurations Reviews	Documented evidence of a review process to ensure Secure Baseline Configurations (SBC) are current and applicable.	CFG-02 CFG-02.5 NET-04 NET-04.1 NET-04.6
26	E-AST-13	Asset Management	Secure Baseline Configurations - Cloud-Based Services	Documented evidence of secure baseline configurations for all deployed types of cloud-based services or applications.	CFG-02 CFG-02.5
27	E-AST-14	Asset Management	Secure Baseline Configurations - Databases	Documented evidence of secure baseline configurations for all deployed types of databases.	CFG-02 CFG-02.5
28	E-AST-15	Asset Management	Secure Baseline Configurations - Embedded Technologies	Documented evidence of secure baseline configurations for all deployed types of embedded technologies.	CFG-02 CFG-02.5
29	E-AST-16	Asset Management	Secure Baseline Configurations - Major Applications	Documented evidence of secure baseline configurations for all deployed types of major applications.	CFG-02 CFG-02.5
30	E-AST-17	Asset Management	Secure Baseline Configurations - Minor Applications	Documented evidence of secure baseline configurations for all deployed types of minor applications.	CFG-02 CFG-02.5
31	E-AST-18	Asset Management	Secure Baseline Configurations - Mobile Devices	Documented evidence of secure baseline configurations for all deployed types of mobile devices.	CFG-02 CFG-02.5
32	E-AST-19	Asset Management	Secure Baseline Configurations - Network Devices	Documented evidence of secure baseline configurations for all deployed types of network devices.	CFG-02 CFG-02.5 NET-04 NET-04.1
33	E-AST-20	Asset Management	Secure Baseline Configurations - Server Class Systems	Documented evidence of secure baseline configurations for all deployed types of server-class operating systems.	CFG-02 CFG-02.5
34	E-AST-21	Asset Management	Secure Baseline Configurations - Workstation Class Systems	Documented evidence of secure baseline configurations for all deployed types of workstation-class operating systems.	CFG-02 CFG-02.5
35	E-AST-22	Asset Management	Provenance	Documented evidence of that tracks the origin, development, ownership, location and changes to systems, system components and associated data.	AST-03.2
36	E-AST-23	Asset Management	Geolocation Inventory	Documented evidence of designated internal and third-party facilities where organizational data is stored, transmitted and/or processed.	BCD-02.4 CLD-09 DCH-19 DCH-24

37	E-AST-24	Asset Management	Asset Categorization	Documented evidence of a methodology to categorize technology assets (e.g., criticality and data classification considerations)	AST-31 AST-31.1
38	E-BCM-01	Business Continuity	Continuity of Operations Plan (COOP)	Documented evidence of a Continuity of Operations Plan (COOP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	BCD-01
39	E-BCM-02	Business Continuity	Recovery Time Objectives (RTOs)	Documented evidence of Recovery Time Objectives (RTOs) that guide Continuity of Operations Plan (COOP)-related operations.	BCD-01.4
40	E-BCM-03	Business Continuity	Recovery Point Objectives (RPOs)	Documented evidence of Recovery Point Objectives (RPOs) that guide Continuity of Operations Plan (COOP)-related operations.	BCD-01.4
41	E-BCM-04	Business Continuity	COOP Root Cause Analysis (RCA)	Documented evidence of a Root Cause Analysis (RCA) from any Continuity of Operations Plan (COOP)-related training, testing or incident.	BCD-05
42	E-BCM-05	Business Continuity	COOP Updates	Documented evidence of a periodic review process for the organization's Continuity of Operations Plan (COOP) to identify necessary updates.	BCD-06
43	E-BCM-06	Business Continuity	COOP Testing	Documented evidence of a Continuity of Operations Plan (COOP)-related testing activity.	BCD-03.1 BCD-04
44	E-BCM-07	Business Continuity	COOP Training	Documented evidence of a Continuity of Operations Plan (COOP)-related training activity.	BCD-03 BCD-04
45	E-BCM-08	Business Continuity	COOP Criticality Analysis	Documented evidence of a Continuity of Operations Plan (COOP)-related criticality analysis.	BCD-02
46	E-BCM-09	Business Continuity	COOP Dependency Analysis	Documented evidence of a Continuity of Operations Plan (COOP)-related dependency analysis for applications, systems, services, facilities, stakeholders and third-parties.	AST-01.1
47	E-BCM-10	Business Continuity	Backups	Documented evidence of a Continuity of Operations Plan (COOP)-related data backup scheme that demonstrates the methods of data backup (including protection measures) for all data types to ensure business continuity requirements.	BCD-11
48	E-BCM-11	Business Continuity	Backups - Local	Documented evidence of event logs for the on-site / local data backup solution.	BCD-11 BCD-11.2
49	E-BCM-12	Business Continuity	Backups - Remote	Documented evidence of event logs for the off-site / remote data backup solution.	BCD-11 BCD-11.2
50	E-BCM-13	Business Continuity	Backups - Recovery	Documented evidence of a Continuity of Operations Plan (COOP)-related criticality analysis for applications, systems, services, facilities, stakeholders and third-parties.	BCD-11 BCD-11.1
51	E-CHG-01	Change Management	Business Impact Analysis (BIA)	Documented evidence of a Business Impact Analysis (BIA) for proposed changes.	RSK-08
52	E-CHG-02	Change Management	Charter - Change Control Board (CCB)	Documented evidence of the organization's Change Control Board (CCB) charter and mission.	CHG-01 CHG-02
53	E-CHG-03	Change Management	Change Control Board (CCB) Minutes	Documented evidence of Change Control Board (CCB) meeting minutes	CHG-02.2
54	E-CHG-04	Change Management	Evidence of Cybersecurity / Data Privacy Reviews	Documented evidence of Change Control Board (CCB) meeting-related cybersecurity and/or privacy reviews for proposed change(s).	CHG-02.3

55	E-CPL-01	Compliance	Statutory, Regulatory & Contractual Obligations	Documented evidence of applicable statutory, regulatory and/or contractual obligations for cybersecurity & data privacy controls.	CPL-01
56	E-CPL-02	Compliance	Defined Compliance Scope (DCS)	Documented evidence of a formal scoping document that identifies applicable statutory, regulatory and/or contractual obligations for the organization. Defines the affected Lines of Business (LOB), internal / external stakeholders and facilities for the specific scope of compliance obligations.	AST-04.1 AST-04.2 AST-04.3 CPL-01.2
57	E-CPL-03	Compliance	Controls Responsibility Matrix (CRM)	Documented evidence of a Controls Responsibility Matrix (CRM), or similar documentation, that identifies the stakeholder involved in executing assigned controls (e.g., Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix).	AST-01.2 AST-03 CLD-06.1 TPM-05.4
58	E-CPL-04	Compliance	Internal Audit (IA)	Documented evidence of an Internal Audit (IA) capability.	CPL-02.1
59	E-CPL-05	Compliance	Internal Audit (IA) Findings	Documented evidence of a centrally-managed and prioritized repository Internal Audit (IA) findings.	CPL-01.1 CPL-03 GOV-01.2
60	E-CPL-06	Compliance	Manufacturer Disclosure Statement for Medical Device Security (MDS2)	Documented Manufacturer Disclosure Statement for Medical Device Security (MDS2) that communicates information about medical device cybersecurity & data privacy characteristics to current device owners and potential buyers. *[note MDS2 is specific to medical device manufacturers]*	TDA-01.1 TDA-02.1 TDA-02.5 TDA-04 TDA-04.1 TPM-04 TPM-04.2
61	E-CPL-07	Compliance	Control Assessments	Documented evidence of internal or third-party control assessments to provide governance oversight of cybersecurity & data privacy controls.	CPL-02 CPL-02.1 CPL-03 CPL-03.1
62	E-CPL-08	Compliance	Functional Review of Cybersecurity Controls	Documented evidence of control testing to ensure cybersecurity controls function as expected.	CPL-03.2
63	E-CPL-09	Compliance	Non-Compliance Oversight Reporting	Documented evidence of governance oversight reporting of non-compliance to the organization's executive leadership.	CPL-02 GOV-01.2
64	E-CRY-01	Cryptographic Protections	FIPS-Validated Certificates	Documented evidence of FIPS-validated cryptographic modules. *[note FIPS-validated cryptography is specific to US government contractors for NIST SP 800-171 & CMMC compliance]*	CRY-03 CRY-04 CRY-09 CRY-09.1 CRY-09.2
65	E-DCH-01	Data Protection	Data Classification Scheme	Documented evidence of an organization-specific data classification scheme.	AST-04.1 DCH-02
66	E-DCH-02	Data Protection	Data Handling Practices	Documented evidence of an organization-specific data handling practices (e.g., guidance specific the data classification scheme).	AST-04.1 DCH-02
67	E-DCH-03	Data Protection	Network Diagram - Global System View (GSV)	Documented evidence of a high-level network diagram that provides a conceptual, logical depiction of the network(s) to describe the interconnections of the systems/applications/services, including internal and external interfaces.	AST-04 NET-02
68	E-DCH-04	Data Protection	Network Diagram - Low Level	Documented evidence of a low-level network diagram that provides a detailed, logical depiction of assets on the network(s).	AST-04 NET-02

69	E-DCH-05	Data Protection	Data Flow Diagram (DFD)	Documented evidence of a Data Flow Diagram (DFD) that accurately identifies where sensitive/regulated data is stored, transmitted and/or processed.	AST-02.8 AST-04 NET-02
70	E-DCH-06	Data Protection	Third-Party Inventories	Documented evidence of an inventory of Third-Party Service Providers (TSP), contractors, vendors, etc. that directly or indirectly impact the organization's data, systems, applications, services and/or processes.	TPM-01.1
71	E-DCH-07	Data Protection	Media Sanitization Documentation	Documented evidence of media sanitization actions.	DCH-09 DCH-09.1
72	E-DCH-08	Data Protection	Authorization Documentation	Documented evidence of that identifies authorized users and processes acting on behalf of authorized users.	CFG-08
73	E-SAT-01	Education	Continuing Professional Education (CPE)	Documented evidence of Continuing Professional Education (CPE) requirements for cybersecurity & data privacy personnel.	SAT-03.7
74	E-SAT-02	Education	Initial User Training	Documented evidence of initial user training for cybersecurity and/or privacy topics.	SAT-02 SAT-02.2 SAT-04 HRS-05.7
75	E-SAT-03	Education	Practical Exercises	Documented evidence of practical user training exercises for cybersecurity and/or privacy topics (e.g., phishing exercise).	SAT-02.1 SAT-03.1 SAT-04
76	E-SAT-04	Education	Recurring User Training	Documented evidence of recurring (e.g., annual) user training for cybersecurity and/or privacy topics.	SAT-03.4 SAT-03.6 SAT-03.7 SAT-04 HRS-05.7
77	E-SAT-05	Education	Role-Based Training	Documented evidence of specialized user training for privileged users, executives, individuals who handle sensitive/regulated data, etc.	SAT-03 SAT-03.4 SAT-03.5 SAT-04
78	E-MON-01	Event Log Monitoring	Evidence of Log Review Processes	Documented evidence of centralized collection and review/analysis of security event logs.	MON-01.2 MON-01.8 MON-02 MON-02.2
79	E-MON-02	Event Log Monitoring	Malware Activity	Documented evidence of malware activity being logged and included as part of the centralized event log collection and review/analysis process.	MON-01.8 MON-02.2 END-04.3
80	E-MON-03	Event Log Monitoring	Privileged User Oversight	Documented evidence of malware activity being logged and included as part of the centralized event log collection and review/analysis process.	MON-01.14 MON-01.15
81	E-MON-04	Event Log Monitoring	Rogue Devices	Documented evidence of rogue device identification is included as part of the centralized event log collection and review/analysis process.	AST-02.6
82	E-MON-05	Event Log Monitoring	Security Events	Documented evidence of security-relevant activities being logged and included as part of the centralized event log collection and review/analysis process.	MON-01.2 MON-01.8 MON-02

					MON-02.2
83	E-HRS-01	Human Resources	Defined Cybersecurity & Data Privacy Roles	Documented evidence of a discrete roles for cybersecurity & data privacy functions (e.g., position categorization).	GOV-04 HRS-02 HRS-03 HRS-03.1
84	E-HRS-02	Human Resources	Assigned Roles - Application Developers	List of employed or contract personnel assigned to application development roles.	HRS-02 HRS-02.1 HRS-03
85	E-HRS-03	Human Resources	Assigned Roles - Cybersecurity Staff	List of employed or contract personnel assigned to cybersecurity roles.	HRS-02 HRS-02.1 HRS-03
86	E-HRS-04	Human Resources	Assigned Roles - Data Privacy Staff	List of employed or contract personnel assigned to data privacy roles.	HRS-02 HRS-02.1 HRS-03
87	E-HRS-05	Human Resources	Role Assignment - CISO	Documented evidence of a formal role assignment to the Chief Information Security Officer (CISO) position.	GOV-04
88	E-HRS-06	Human Resources	Role Assignment - COO	Documented evidence of a formal role assignment to the Chief Operations Officer (COO) position.	GOV-04
89	E-HRS-07	Human Resources	Role Assignment - CIO	Documented evidence of a formal role assignment to the Chief Information Officer (CIO) position.	GOV-04
90	E-HRS-08	Human Resources	Role Assignment - CPO	Documented evidence of a formal role assignment to the Chief Privacy Officer (CPO) position.	GOV-04 PRI-01.1
91	E-HRS-09	Human Resources	Role Assignment - CRO	Documented evidence of a formal role assignment to the Chief Risk Officer (CRO) position.	GOV-04
92	E-HRS-10	Human Resources	Role Assignment - DPO	Documented evidence of a formal role assignment to Data Protection Officer (DPO) positions.	GOV-04 PRI-01.4
93	E-HRS-11	Human Resources	Role Assignment - Sensitive / Regulated Data	Documented evidence of a formal role assignment to personnel who are cleared to handle sensitive/regulated data.	HRS-02 HRS-02.1 HRS-03
94	E-HRS-12	Human Resources	Role Review	Documented evidence of a formal review process to ensure personnel roles currently reflect business needs.	IAC-07 IAC-07.1 IAC-08 IAC-17
95	E-HRS-13	Human Resources	Defined Cybersecurity & Data Privacy Responsibilities	Documented evidence of a role-based cybersecurity & data privacy responsibilities to ensure personnel are both educated on the role and are responsible for the associated control execution.	GOV-04 HRS-03 HRS-03.1
96	E-HRS-14	Human Resources	Responsibilities Review	Documented evidence of a formal review process to ensure assigned responsibilities currently reflect business needs for the assigned role.	IAC-17
97	E-HRS-15	Human Resources	Organization Chart	Current and accurate organization chart that depicts logical staff hierarchies.	GOV-04 GOV-04.1 GOV-04.2
98	E-HRS-16	Human Resources	Access Agreements	Documented evidence of personnel management practices protecting sensitive/regulated data through formal access agreements.	HRS-03.1 HRS-05 HRS-06 HRS-10
99	E-HRS-17	Human Resources	Background Checks	Documented evidence of personnel screening practices, which centers around some form of formalized background check process.	HRS-04 HRS-04.1

100	E-HRS-18	Human Resources	Provisioning Checklist (Onboarding)	Documented evidence of personnel management practices to formally onboard personnel into their assigned roles.	HRS-03 HRS-03.1 HRS-04.2 HRS-05.7 HRS-10 IAC-07
101	E-HRS-19	Human Resources	Deprovisioning Checklist (Offboarding)	Documented evidence of personnel management practices to formally offboard personnel from their assigned roles due to employment termination or role change.	HRS-06.2 HRS-09 HRS-09.1 HRS-09.2 HRS-09.3 IAC-07 IAC-07.1 IAC-07.2
102	E-HRS-20	Human Resources	Non-Disclosure Agreements (NDAs)	Documented evidence of the use of Non-Disclosure Agreements (NDAs) that restricts unauthorized sharing of sensitive/regulated data.	HRS-06.1
103	E-HRS-21	Human Resources	Position Competency Requirements	Documented evidence of personnel management practices to define minimum competency requirements for cybersecurity & data privacy-related roles.	HRS-03.2 HRS-04 HRS-04.1
104	E-HRS-22	Human Resources	Rules of Behavior	Documented evidence of personnel management practices to define "acceptable use" or "rules of behavior" criteria that specify acceptable and unacceptable user behaviors.	HRS-02 HRS-02.1 HRS-03 HRS-05 HRS-05.1 HRS-05.2 HRS-05.3 HRS-05.4 HRS-05.5 HRS-10
105	E-HRS-23	Human Resources	Critical Cybersecurity & Data Privacy Skills	Documented evidence of personnel management practices to formally identify critical cybersecurity skills needed to support business operations.	HRS-03.2 HRS-13
106	E-HRS-24	Human Resources	Critical Cybersecurity & Data Privacy Skill Gaps	Documented evidence of personnel management practices to formally identify critical cybersecurity skill gaps.	HRS-13 HRS-13.1
107	E-HRS-25	Human Resources	Separation of Duties (SoD)	Documented evidence of personnel management practices to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	HRS-11 HRS-12
108	E-HRS-26	Human Resources	Vital Cybersecurity & Data Privacy Staff	Documented evidence of personnel management practices to formally identify vital cybersecurity & data privacy personnel.	HRS-13.2
109	E-IAM-01	Identity & Access Management	Access Permission Review	Documented evidence of periodic access permission reviews.	IAC-17
110	E-IAM-02	Identity & Access Management	Defined Roles (RBAC)	Documented evidence of defined access control-specific roles (e.g., Role Based Access Control (RBAC)).	IAC-08
111	E-IAM-03	Identity & Access Management	Privileged User Inventory	Documented evidence of an inventory of privileged users across systems, applications and services (internal and external).	IAC-16 IAC-16.1

112	E-IRO-01	Incident Response	Incident Response Program (IRP)	Documented evidence of a Incident Response Plan (IRP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	IRO-04
113	E-IRO-02	Incident Response	Indicators of Compromise (IOC)	Documented evidence of defined Indicators of Compromise (IOC).	IRO-03
114	E-IRO-03	Incident Response	Incident Tracking	Documented evidence of a centralized repository to track cybersecurity & data privacy incidents.	IRO-02 IRO-09
115	E-IRO-04	Incident Response	IRP Testing	Documented evidence of an Incident Response Plan (IRP)-related testing activity.	IRO-06
116	E-IRO-05	Incident Response	Table Top Exercises	Documented evidence of "table top" exercises that test incident response practices.	IRO-05
117	E-IRO-06	Incident Response	IRP Training	Documented evidence of an Incident Response Plan (IRP)-related training activity.	IRO-05
118	E-IRO-07	Incident Response	IRP Updates	Documented evidence of a periodic review process for the organization's Incident Response Plan (IRP) to identify necessary updates.	IRO-04.2
119	E-IRO-08	Incident Response	Root Cause Analysis (RCA)	Documented evidence of a Root Cause Analysis (RCA) from any Incident Response Plan (IRP)-related training, testing or incident.	IRO-13
120	E-IAO-01	Information Assurance	Information Assurance Program (IAP)	Documented evidence of a Information Assurance Program (IAP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	IAO-01
121	E-IAO-02	Information Assurance	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	Documented evidence of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable AI-related testing, identification of incidents and information sharing.	AAT-10
122	E-MNT-01	Maintenance	Maintenance - Authorized Maintenance Personnel	Documented evidence of personnel who have designated maintenance roles.	MNT-06.1
123	E-MNT-02	Maintenance	Maintenance Plan	Documented evidence of a Maintenance Plan. This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	MNT-01
124	E-MNT-03	Maintenance	Patch Management	Documented evidence of maintenance activities for systems, applications and services management (e.g., patch management).	VPM-01 VPM-04 VPM-05
125	E-MNT-04	Maintenance	Infrastructure Maintenance	Documented evidence of maintenance activities for the organization's infrastructure and supporting systems.	MNT-01 MNT-02 MNT-03 MNT-03.1
126	E-NET-01	Network Security	Content / DNS Filtering	Documented evidence of the methods that content / DNS filtering is implemented to prevent Internet traffic from prohibited content and/or hostile web sites.	NET-18 NET-18.1
127	E-NET-02	Network Security	Wireless Rogue Detection	Documented evidence of automated or manual means to detect rogue wireless devices.	NET-15.5
128	E-NET-03	Network Security	Work From Anywhere (WFA)	Documented evidence of administrative and technical measures that are enforced at "alternate work sites"	NET-14 NET-14.5

			Guidance (remote workers)	which includes working from home or working while traveling on business.	
129	E-PES-01	Physical Security	Environmental Monitoring	Documented evidence of environmental monitoring (e.g., water leaks, temperature, humidity, etc.)	PES-01 PES-07 PES-08 PES-09
130	E-PES-02	Physical Security	Visitor Logbook	Documented evidence of a visitor management and logging visitor activities.	PES-03 PES-03.3 PES-06 PES-06.4
131	E-PES-03	Physical Security	Defined Physical Security Roles	Documented evidence of defined physical access control-specific roles that limit physical access to rooms and/or facilities.	PES-02 PES-02.1
132	E-PES-04	Physical Security	Site Security Plan (Site Plan)	Documented evidence of a site security plan (site plan).	PES-01.1
133	E-PRI-01	Privacy	Accounting of Disclosures	Documented evidence of accounting for privacy-related disclosures.	PRI-14.1
134	E-PRI-02	Privacy	Authorized Use	Documented evidence of authorized use definitions for privacy-related data operations.	PRI-04 PRI-04.1 PRI-05 PRI-05.1
135	E-PRI-03	Privacy	Data Authority Registrations	Documented evidence of registrations made with applicable data authorities for privacy-related data processing.	PRI-15
136	E-PRI-04	Privacy	Data Protection Impact Assessment (DPIA)	Documented evidence of Data Protection Impact Assessment (DPIA).	RSK-10
137	E-PRI-05	Privacy	Data Sharing Agreement	Documented evidence of formal data sharing practices that address, at a minimum: • The business justification for the data sharing; • The type / category of data being shared; • The third-parties the data is being shared with; • Lawful bases for data sharing; and • Data subject rights.	PRI-01.5 PRI-07 PRI-07.1 PRI-07.2
138	E-PRI-06	Privacy	Data Subject Access	Documented evidence of how data subject access requests are handled that includes intake through remediation.	PRI-06
139	E-PRI-07	Privacy	Personal Data Categories	Documented evidence of formal personal data categories.	PRI-05.7
140	E-PRI-08	Privacy	Privacy Notice	Documented evidence of a publicly-accessible privacy notice.	PRI-02
141	E-PRM-01	Resource Management	Cybersecurity Business Plan (CBP)	Documented evidence of a cybersecurity-specific business plan that documents a strategic plan and discrete objectives.	GOV-08 PRM-01.1 PRM-03
142	E-PRM-02	Resource Management	Portfolio Roadmap	Documented evidence of the organization's roadmap for implementing cybersecurity-related initiatives and technologies.	PRM-01 PRM-02 PRM-03
143	E-PRM-03	Resource Management	Secure Development Lifecycle (SDLC)	Documented evidence of a secure development lifecycle that the organization utilizes for new initiatives or significant changes to existing initiatives to ensure cybersecurity & data privacy principles are identified and implemented by default.	PRM-04 PRM-05 PRM-06 PRM-07
144	E-PRM-04	Resource Management	Targeted Maturity Level	Documented evidence of a targeted level of control maturity from a Capability Maturity Model (CMM).	PRM-01.2

145	E-RSK-01	Risk Management	Risk Management Program (RMP)	Documented evidence of a Risk Management Program (RMP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	RSK-01
146	E-RSK-02	Risk Management	Cybersecurity Supply Chain Risk Management (C-SCRM)	Documented evidence of a Cybersecurity Supply Chain Risk Management (C-SCRM). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	RSK-09 TPM-03
147	E-RSK-03	Risk Management	Plan of Actions & Milestones (POA&M) / Risk Register	Documented evidence of a POA&M, or risk register, that tracks control deficiencies from identification through remediation.	AST-02.4 CPL-02 RSK-04.1
148	E-RSK-04	Risk Management	Cybersecurity Risk Assessment (RA)	Documented evidence of a cybersecurity-specific risk assessment.	RSK-04
149	E-RSK-05	Risk Management	Supply Chain Risk Assessment (SCRA)	Documented evidence of supply chain-specific risk assessment that evaluates risks that are specific to its supply chain.	RSK-09.1
150	E-RSK-06	Risk Management	Risk Threshold	Documented evidence the organization has a defined risk threshold.	RSK-01.3
151	E-RSK-07	Risk Management	Risk Tolerance	Documented evidence the organization has a defined risk tolerance.	RSK-01.4
152	E-RSK-08	Risk Management	Risk Appetitie	Documented evidence the organization has a defined risk appetite.	RSK-01.5
153	E-TDA-01	Technology Design & Acquisition	Secure Software Development Principles (SSDP)	Documented evidence of a Secure Software Development Principles (SSDP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	SEA-01 TDA-01
154	E-TDA-02	Technology Design & Acquisition	Secure Engineering & Data Privacy (SEDP)	Documented evidence of a Secure Engineering & Data Privacy (SEDP) program. This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	SEA-01 TDA-01
155	E-TDA-03	Technology Design & Acquisition	Application Security Testing (AST)	Documented evidence of application security testing (e.g., DAST, SAST, fuzzing, etc.).	TDA-06.2 TDA-09 TDA-09.1 TDA-09.2 TDA-09.3 TDA-09.4 TDA-09.5 TDA-09.6
156	E-TDA-04	Technology Design & Acquisition	Design and Development Plan (DDP)	Documented evidence of an engineering method to control the design process and govern the lifecycle of the product/service.	SEA-01 SEA-02 SEA-03 TDA-02.3 TDA-05 TDA-06.3
157	E-TDA-05	Technology Design & Acquisition	Failure Mode and Effect Analysis (FMEA)	Documented evidence of an engineering method designed to define, identify, and present solutions for system failures, problems, or errors.	TDA-01.1 TDA-06.5 TDA-09

158	E-TDA-06	Technology Design & Acquisition	Multi Patient Harm View (MPHV)	Documented evidence of a description of a Multi Patient Harm View (MPHV) that explains how the device / system defends against and/or responds to attacks with the potential to harm multiple patients. *[note MPHV is specific to medical device manufacturers]*	TDA-01.1 TDA-02 TDA-04 TDA-04.1
159	E-TDA-07	Technology Design & Acquisition	Ports, Protocols & Services (PPS)	Documented evidence of all ports, protocols and services in use by the system, application or service.	TDA-01.1 TDA-02.1 TDA-02.5 TPM-04.2
160	E-TDA-08	Technology Design & Acquisition	Secure Engineering Principles (SEP)	Documented evidence of defined secure engineering principles used to ensure Confidentiality, Integrity, Availability & Safety (CIAS) concerns are properly addressed in the design and implementation of systems, applications and services.	SEA-01 TDA-01 TDA-06
161	E-TDA-09	Technology Design & Acquisition	Security Architecture View	Documented evidence that identifies security-relevant system elements and their interfaces: • Define security context, domains, boundaries, and external interfaces of the system; • Align the architecture with (a) the system security objectives and requirements, (b) security design characteristics; and • Establish traceability of architecture elements to user and system security requirements.	CLD-02 SEA-01 SEA-02 SEA-03
162	E-TDA-10	Technology Design & Acquisition	Security Use Case View (SUCV)	Documented evidence of diagrams, with explanatory text, describing various security scenarios in each of the operational and clinical functionality states of the system and how the system addresses each scenario architecturally. *[note SUCV is specific to medical device manufacturers]*	TDA-04 TDA-04.1 TDA-06.2
163	E-TDA-11	Technology Design & Acquisition	Software Assurance Maturity Model (SAMM)	Documented evidence of a Software Assurance Maturity Model (SAMM).	TDA-06 TDA-06.3
164	E-TDA-12	Technology Design & Acquisition	Software Bill of Materials (SBOM)	Documented evidence of a Software Bill of Materials (SBOM).	TDA-04.2
165	E-TDA-13	Technology Design & Acquisition	Software Escrow	Documented evidence of a software escrow solution.	TDA-20.3
166	E-TDA-14	Technology Design & Acquisition	System Security & Privacy Plan (SSPP)	Documented evidence of at least one (1) System Security Plan (SSPP) that covers the sensitive/regulated data environment. There may be multiple SSPPs, based on applicable contracts.	AST-02.4 IAO-03
167	E-TDA-15	Technology Design & Acquisition	Updateability / Patchability View	Documented evidence of a description of the end-to-end process permitting software updates and patches to be deployed to the device/service.	TDA-01.1 TDA-01.2 TDA-04.1
168	E-TDA-16	Technology Design & Acquisition	Vulnerability Disclosure Program (VDP)	Documented evidence of a Vulnerability Disclosure Program (VDP) (e.g., bug bounty).	THR-06
169	E-THR-01	Threat Management	Indicators of Exposure (IOE)	Documented evidence of defined Indicators of Exposure (IOE).	THR-02
170	E-THR-02	Threat Management	Industry Associations / Memberships	Documented evidence of industry associations the organization utilizes to maintain situational awareness of evolving threats and trends.	GOV-07

171	E-THR-03	Threat Management	Threat Intelligence Feeds (TIF)	Documented evidence of threat intelligence feeds.	THR-03
172	E-THR-04	Threat Management	Threat Intelligence Program (TIP)	Documented evidence of a formal capability that intakes and analysis threat information to determine specific threat to the organization and necessary actions to mitigate the threat(s).	THR-01 THR-04
173	E-THR-05	Threat Management	Threat Mitigation	Documented evidence of steps taken to mitigate identified threats.	TDA-06.2 THR-07 VPM-01 VPM-04
174	E-TPM-01	Third-Party Management	Third-Party Contracts	Documented evidence of third-party contractual obligations for cybersecurity & data privacy protections.	TPM-01 TPM-05 PRI-07 PRI-07.1 PRI-07.2
175	E-TPM-02	Third-Party Management	Third-Party Criticality Assessment	Documented evidence of third-party criticality assessment that evaluates the critical nature of each third-party the organization works with.	TPM-02
176	E-TPM-03	Third-Party Management	Third-Party Service Reviews	Documented evidence of a formal, annual stakeholder review of third-party services for each Third-Party Service Provider (TSP).	TPM-01 TPM-05 TPM-05.5 TPM-08 TPM-09
177	E-TPM-04	Third-Party Management	Service Level Agreements (SLAs)	Documented evidence of third-party Service Level Agreements (SLAs) to support business operations.	BCD-09.3 BCD-10.1 OPS-03
178	E-TPM-05	Third-Party Management	Break Clauses	Documented evidence of "break clauses" in third-party contracts.	TPM-05.7
179	E-VPM-01	Vulnerability & Patch Management	Vulnerability & Patch Management Program (VPMP)	Documented evidence of a Vulnerability & Patch Management Program (VPMP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	VPM-01
180	E-VPM-02	Vulnerability Management	Penetration Testing - Application	Documented evidence of Application Security Testing (AST) activities: • Abuse case, malformed, and unexpected inputs (e.g., Robustness or Fuzz testing); • Attack surface analysis; • Vulnerability chaining; • Closed box testing of known vulnerability scanning; • Software composition analysis of binary executable files; and/or • Static and dynamic code analysis, including testing for credentials that are “hardcoded,” default, easily guessed, and easily compromised.	VPM-07
181	E-VPM-03	Vulnerability Management	Penetration Testing - Network	Documented evidence of internal and external network penetration testing activities that focus on discovering and exploiting security vulnerabilities.	VPM-07
182	E-VPM-04	Vulnerability Management	Red Team Testing	Documented evidence of "red team" testing.	VPM-07.1
183	E-VPM-05	Vulnerability Management	Vulnerability Assessments	Documented evidence of internal and external vulnerability assessment activities.	VPM-06 VPM-06.6 VPM-06.7