SECURE CONTROLS FRAMEWORK CONFORMITY ASSESSMENT PROGRAM (SCF CAP)

HIPAA SECURITY RULE (NIST SP 800-66 R2) THIRD-PARTY ASSESSMENT, ATTESTATION & CERTIFICATION (3PAAC) GUIDE & STANDARDS

Version 1.3
March 2026

This publication is available free of charge from: **https://content.securecontrolsframework.com/cap/ag-hipaa-security.pdf**

Table of Contents

INTRODUCTION

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

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

SCF CONFORMITY ASSESSMENT PROGRAM (SCF CAP) OVERVIEW

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

The SCF Council established the Secure Controls Framework Conformity Assessment Program (SCF CAP) as a structure to conduct cybersecurity and data protection-related Third-Party Assessment, Attestation and Certification Services (SCF 3PAAC Services).[4] There is a need for a scalable, cost-effective solution to obtain a company-level, third-party assessment of security, compliance and resilience practices and the SCF CAP addresses that need.

The SCF CAP exists to leverage SCF content to provide a company-level certification through a conformity assessment process. The SCF CAP is designed to make conformity assessments more cost-effective, efficient and objective through the use of the SCF's metaframework structure and no-cost content.

As a metaframework, the SCF CAP allows for a singular certification approach to security, compliance and resilience requirements where it:

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

The SCF CAP:

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

The SCF CAP BoK provides details on the SCF Certification process, including criteria necessary to obtain a **SCF Certified™ - HIPAA Security Rule** certification.

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

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

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

- Assessment: The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for an information system or organization.[6]
- Attestation: The issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated.[7]
- Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.[8]

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

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

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

Normative References

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

(1) NIST Cybersecurity Framework (NIST CSF) version 2.0;[9]
(2) NIST IR 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings*;[10]
(3) SCF published Set Theory Relationship Mapping (STRM) for HIPAA Security Rule;[11]
(4) Cybersecurity & Data Protection Assessment Standards (CDPAS);[12] and
(5) SCF Conformity Assessment Program Body of Knowledge (SCF CAP BoK).[13]

Intended Audience

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

- OSA;
- Third-Party Assessment Organizations (SCF 3PAOs);
- SCF Assessors; and
- External Service Providers (ESP):
  - Consultants;
  - Cloud Service Providers (CSP);
  - Managed Service Providers (MSP); and
  - Managed Security Services Providers (MSSP).

[6] *NIST Glossary for Assessment - https://csrc.nist.gov/glossary/term/assessment*
[7] *NIST Glossary for Attestation - https://csrc.nist.gov/glossary/term/attestation*
[8] *NIST Glossary for Certification - https://csrc.nist.gov/glossary/term/certification*
[9] *HIPAA Security Rule download - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf*
[10] *NIST IR 8477 - https://csrc.nist.gov/pubs/ir/8477/final*
[11] *SCF STRM for HIPAA Security Rule - https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-law-hipaa-simplification-2013.pdf*
[12] *SCF CDPAS – https://content.securecontrolsframework.com/pdf/cdpas.pdf*
[13] *SCF CAP Body of Knowledge – https://content.securecontrolsframework.com//cap/scf-cap-bok.pdf*

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

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

Assessment Scoping

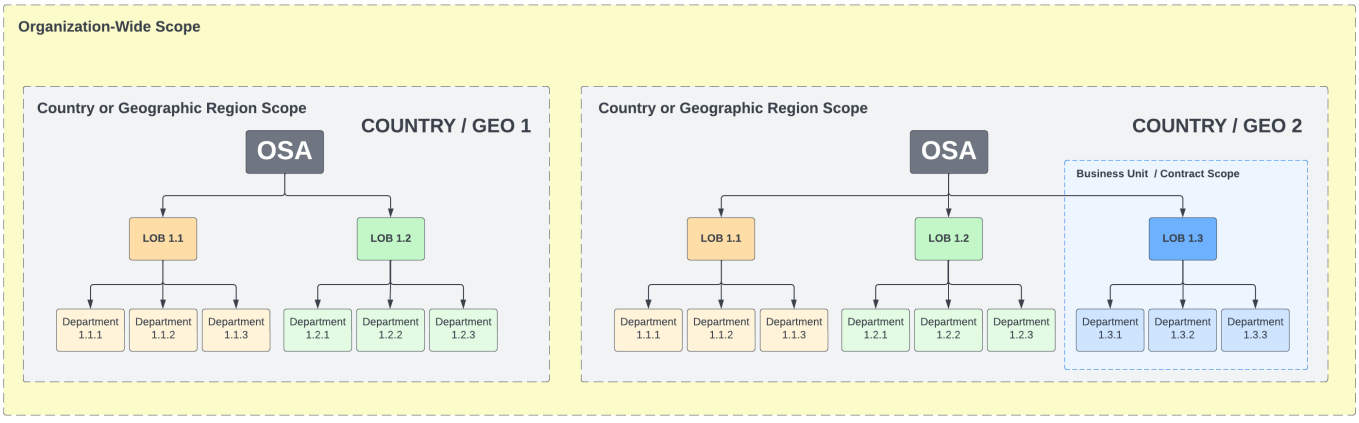
The SFC Council recognizes the Unified Scoping Guide (USG) as the authoritative guidance for determining scope.[14] Prior to engaging a SCF 3PAO for SCF 3PAAC Services, the OSA must specify the assessment scope. The assessment boundary demarcation can be defined as one (1) of the following four (4) scoping options:

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

To define the demarcation of the assessment boundary:

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

A graphical representation of this assessment scoping is shown below:



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

UPDATES

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

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

Errata will be provided to indicate:

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

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

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

LIABILITY LIMITATIONS

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

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

TERMINOLOGY & ACRONYMS

The SCF Council recognizes two (2) primary sources for authoritative definitions for security, compliance and resilience-related terminology:

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define cybersecurity-related terminology;[15] and
- NIST Glossary.[16]

TERMINOLOGY STANDARDIZATION

From the context of applying a standard to SCF 3PAAC Services, it is important to clarify mandatory versus optional criteria:[17]

- The terms "*SHALL*" and "*SHALL NOT*" indicate requirements:
  - To be followed strictly in order to conform; and
  - From which no deviation is permitted.
- The terms "*SHOULD*" and "*SHOULD NOT*" indicate that:
  - Among several possibilities one (1) is recommended as particularly suitable, without mentioning or excluding others;
  - A certain course of action is preferred, but not necessarily required; or
  - A certain possibility, or course of action, is discouraged, but not prohibited.
- The terms "MAY" and "NEED NOT" indicate a course of action permissible within reasonable limits.
- The terms "*CAN*" and "*CANNOT*" indicate:
  - A possibility and capability; or
  - The absence of that possibility or capability.

SCF Council Guidance: Within the cybersecurity profession, the term "control" can be applied to a variety of contexts and can serve multiple purposes. When used in the SCF CAP context, a control is a mechanism (e.g., a safeguard or countermeasure) designed to address protection needs specified by an entity's requirements.

- *Controls are:*
  - *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; and/or*
  - *A device or mechanism used to regulate or guide the operation of a machine, apparatus or system.*
- *Requirements are statements that translate, or express, a need and its associated constraints and conditions.*

Additional clarification for assessment-relevant terminology:

- Assessment Boundary. The scope of an organization's control implementation to which assessment of objects is applied:
  - An assessment may involve multiple assessment boundaries; and
  - Assessment boundary may be defined as the People, Processes, Technologies, Data and/or Facilities (PPTDF) that comprise:
    - The entire organization;
    - A specific contract, project or initiative;
    - A specific Business Unit (BU) within an organization; or
    - A specific country, or geographic region, of the organization's business operations.
- Assessment Object. The item (e.g., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
- Assurance. Grounds for justified confidence that a security or privacy claim has been or will be achieved. [18]
- Compensating Control. Alternative cybersecurity and/or data protection controls implemented in lieu of the deficient control that provide equivalent or comparable protection. Compensating controls:

[15] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*
[16] *NIST Glossary - https://csrc.nist.gov/glossary*
[17] *NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html*
[18] *NIST Glossary for Assurance - https://csrc.nist.gov/glossary/term/assurance*

- Include physical, administrative and/or technical safeguards or countermeasures employed by an organization in lieu of the deficient control; and
- Reduce risk to the affected system(s), service(s), application(s), service(s), individual(s) and/or organization(s) in a manner that is equivalent to, or comparable to, the protection offered if the deficient control was operational and effective.

- Conformity Assessment. A demonstration that specified requirements are fulfilled. To learn more about conformity assessments, NIST published Special Publication 2000-01, *ABC's of Conformity Assessment*, that serves as a worthwhile primer on the subject.[19]
- Control Inheritance: Security control inheritance is a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.[20]
- Due Care. The standard of care where a reasonable person would exercise in the same situation or under similar circumstances. This standard of care is used in a tort action to determine whether a person was negligent.[21]
- Due Diligence. The level of reasonable care or attention expected to avoid liability.[22]
- Implemented Capability. An implemented capability is a technical, administrative or physical mechanism that exists in a production environment and can demonstrate reasonable effectiveness.
- Material Control. When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. A material control is such a fundamental cybersecurity and/or data privacy control that:
  - It is not capable of having compensating controls; and
  - Its absence, or failure, exposes an organization to such a degree that it could have a material impact.
- Material Risk. When an identified risk that poses a material impact, that is a material risk.
  - A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
  - A material risk should be identified and documented in an organization's "risk catalog" that chronicles the organization's relevant and plausible risks.
- Material Threat. When an identified threat poses a material impact, that is a material threat.
  - A material threat is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
  - A material threat should be identified and documented in an organization's "threat catalog" that chronicles the organization's relevant and plausible threats.
- Material Incident. When an incident poses a material impact, that is a material incident.
  - A material incident is an occurrence that does or has the potential to:
    - Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the organization; and/or
    - Constitute a violation, or imminent threat of violation, of an organization's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).
  - Reasonably foreseeable material incidents should be documented in an organization's Incident Response Plan (IRP) that chronicles the organization's relevant and plausible incidents, so there are appropriate practices to identify, respond to and recover from such incidents.
- Material Weakness. A material weakness is a deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data privacy 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.
  - When there is an existing deficiency (e.g., control deficiency) that poses a material impact, that is a material weakness (e.g., inability to maintain access control, lack of situational awareness to enable the timely identification and response to incidents, etc.).

[19] *NIST SP 2000-1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.2000-01.pdf*
[20] *NIST Glossary for Security Control Inheritance - https://csrc.nist.gov/glossary/term/security_control_inheritance*
[21] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_care*
[22] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_diligence*

- A material weakness will be identified as part of a gap assessment, audit or other form of assessment as a finding due to one (1), or more, control deficiencies. A material weakness should be documented in an organization's Plan of Action & Milestones (POA&M), risk register, or similar tracking mechanism for remediation purposes.

- Mechanism. A mechanism can be described as a: [23]
  - Process or system that is used to produce a particular result; or
  - Device or method for achieving a security-relevant purpose.
- Reciprocity. Reciprocity is an agreement among participating organizations to accept each other's: [24]
  - Security assessments to reuse system resources; and/or
  - Assessed security posture to share information.
- Risk. A risk is:
  - A situation where someone, or something valued, is exposed to danger, harm or loss (noun); or
  - To expose someone or something valued to danger, harm or loss (verb).
- Risk Appetite: The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. [25]
- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result. [26]
- Risk Threshold: Values used to establish concrete decision points and operational control limits to trigger management action and response escalation. [27]
- Security. A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach. [28]
- Threat. A threat:
  - Is a person, or thing, likely to cause damage or danger (noun); or
  - Indicates impending damage or danger (verb).
- Trust. A belief that an entity meets certain expectations and therefore, can be relied upon. [29]

Acronyms

The following acronyms are used throughout the assessment guide:

Acronym	Term	Definition
1PD	First Party Declaration	1PDs are self-attestations.
3PA	Third-Party Attestation	3PA are attestations made by a third-party, generally in the performance of an assessment or audit.
3PAAC Services	Third-Party Assessment, Attestation and Certification Services	Assessment, attestation and certification services performed by a third-party organization.
SCF 3PAO	Third-Party Assessment Organization	A company that performs assessment, attestation and certification services.
AAT	Artificial Intelligence and Autonomous Technologies	Tools that are advanced enough to act with limited human involvement through Artificial Intelligence (AI), Machine Learning (ML) or similar autonomous technologies.
AO	Assessment Objective	AOs are objective statements that establish the purpose and intended outcome of the assessment for a specific control. There may be multiple AOs associated with a control.
APIT	Automated Point In Time	APIT assessments utilize automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity

[23] *NIST Glossary for Mechanism - https://csrc.nist.gov/glossary/term/mechanism*
[24] *NIST Glossary for Reciprocity - https://csrc.nist.gov/glossary/term/reciprocity*
[25] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*
[26] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*
[27] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*
[28] *NIST Glossary for Security - https://csrc.nist.gov/glossary/term/security*
[29] *NIST Glossary for Trust - https://csrc.nist.gov/glossary/term/trust*

		versus the current state via machine-readable configurations and/or assessment evidence: ▪ Relevant to a specific point in time (time at which the control was evaluated); ▪ In situations where technology cannot evaluate evidence, evidence is manually reviewed; and ▪ The combined output of automated and manual reviews of artifacts is used to derive a finding.
ATE	Assessment Technical Expert	ATE are assessment team members who have the necessary subject matters expertise to conduct a specific part of an assessment. ATE report to the ATL.
ATL	Assessment Team Lead	An ATL is an individual assigned by the SCF 3PAO to lead the assessment team in the conduct of SCF 3PAAC Services.
AEHR	Automated Evidence with Human Assessment	AEHR assessments are used for ongoing, continuous control assessments: ▪ AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and ▪ Recurring human reviews: ○ Evaluate the legitimacy of the results from automated control assessments; and ○ Validate the automated evidence review process to derive a finding.
CDPAS	Cybersecurity & Data Protection Assessment Standards	A cohesive, consistent set of standards to govern cybersecurity and data protection related 3PAAC Services.
CIAS	Confidentiality, Integrity, Availability and/or Safety	CIAS is an evolution of the "CIA Triad" concept that defines the purpose of security controls. It adds the component of Safety.
COI	Conflict of Interest	COI involves situations in which a personal interest, or relationship, conflicts with the faithful performance of an official duty.
CICA	Continuous Incremental Conformity Assessment	An incremental approach to performing "continuous" compliance assessments that relies on recurring control assessments over a period of time.
CVC	Conformity Validation Cadence	The cadence at which the evidence of control function are evaluated (e.g., daily, weekly, monthly, quarterly, semi-annual or annual).
CPE	Continuing Professional Education	CPE describes the ongoing process of improving skills and competencies through formal or informal educational activities.
DSR	Discretionary Security Requirements	DSR are discretionary cybersecurity and/or data privacy controls that address voluntary industry practices or internal requirements. DSR are primarily internally influenced, based on the organization's respective industry and risk tolerance.
ERL	Evidence Request List	ERLs establish a finite list of supporting evidence used in an assessment: ▪ Prior to the start of the assessment, an ERL is provided by the SCF 3PAO to the OSA. ▪ The ERL's standardized evidence expectations allow OSAs to have sufficient time to accumulate reasonable evidence to determine the adequacy of control design and operation.
ESP	External Service Provider	An independent, third-party organization that provides services, technologies, facilities and/or people. ESPs include but are not limited to: ▪ Consulting / professional services; ▪ Software development; ▪ Staff augmentation; and ▪ Technology support (e.g., Managed Services Provider (MSP)).
HMI	Human-Machine Interface	HMI consists of software and/or interfaces that monitors and/or sends commands to controllers within an ICS.
IaaS	Infrastructure as a Service	IaaS is a cloud computing model that delivers on-demand, virtualized computing resources (e.g., servers, storage, networking, etc.). The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
IC	Implemented Capability	IC refer to technical, administrative and physical controls where:

		▪ Technology capabilities will only be considered implemented if the system(s), application(s) and/or service(s) has/have been operational in a production environment for at least sixty (60) days; ▪ Administrative processes will only be considered implemented if there is evidence to demonstrate that process has been: o Used in a real-world situation (e.g., onboarding/offboarding personnel, incident response, etc.); and/or o Formally tested (e.g., documented incident response exercise); and ▪ Physical capabilities will only be considered implemented if the physical security mechanism(s) has/have been operational in a production environment for at least thirty (30) days.
ICS	Industrial Control Systems	ICS are a type of OT. An ICS is broader system of technologies that includes PLCs, sensors and networks.
IoT	Internet of Things	IoT refers to Internet-enabled technologies (e.g., smart devices) that can provide monitoring and automation tasks.
MCR	Minimum Compliance Requirements	MCR are minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations.
ML	Machine Learning	ML is a subset of AI that enables systems to earn from large data sets to identify patterns and make predictions without being explicitly programmed for every specific task.
MLC	Maturity Level Criteria	MLC are specific to each maturity level to define reasonable staffing, technologies and processes to implement the desired level of maturity.
MPIT	Manual Point In Time	MPIT is a traditional assessment methodology that: ▪ Is relevant to a specific point in time (time at which the control was evaluated); and ▪ Relies on the manual review of artifacts to derive a finding.
MSA	Master Services Agreement	MSAs are comprehensive contracts between two parties that establish terms and conditions of current and future transactions.
OSA	Organization(s) Seeking Assessment	A company, entity or business unit seeking the external assessment.
OT	Operational Technology	OT encompasses systems that detect and/or cause direct changes in the physical world by monitoring and controlling assets and processes (e.g., industrial technologies).
PaaS	Platform as a Service	IaaS is a cloud computing model that provides pre-configured tools, databases and middleware as a platform that enables consumers to build, deploy and manage applications. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
PbD	Privacy by Design	Data privacy through the design and governance of processes and technologies. PbD prioritizes data protection as a core business requirement, rather than a technical feature.
PLC	Programmable Logic Controller	PLCs are a type of IT. PLCs are “ruggedized” technologies that are designed for industrial settings to automate manufacturing processes, machineries and/or industrial systems.
RASCI	Responsible, Accountable, Supportive, Consulted & Informed	Refers to a RASCI matrix that defines responsibilities associated with individuals or teams: ▪ Responsible - entity directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task; ▪ Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and

		▪ Informed - entity(ies) not involved in task execution but are informed when the task is completed.
ROC	Report on Conformity	A formalized report that issues an assessment determination statement. The ROC summarizes the assessment findings.
SaaS	Software as a Service	SaaS is a cloud computing model that offers software and/or services on a subscription bases, accessed over the Internet.
SbD	Secure by Design	Processes and technologies are designed and built in a way that protects against reasonable threats. SbD prioritizes cybersecurity as a core business requirement, rather than treating it as a technical feature.
SCADA	Supervisory Control and Data Acquisition	SCADA is a type of OT. It is a Human-Machine Interface (HMI) for operators to monitor, control and adjust physical industrial processes in real-time.
SCF	Secure Controls Framework	A community driven metaframework that contains over 1.400 controls spanning over 200 cybersecurity and data privacy laws, regulations and frameworks.
SCR	Security, Compliance & Resilience	Refers to the three (3) key components of the SCF's Security, Compliance & Resilience Management System (SCRMS).
SOW	Statement of Work	SOWs are contracts that cover the work management aspects of a project (e.g., scope, timeline, cost, responsibilities, etc.).

SCF CAP Assessment Criteria Overview

The SCF CAP is designed to be objective and assess an organization based on the merits of its cybersecurity and data protection program. The SCF CAP uses standardized terminology to clearly indicate status:

- At the control-level, the SCF CAP assigns a control designation; and
- At the assessment boundary-level, the SCF CAP assigns an assessment conformity designation (e.g., certification).

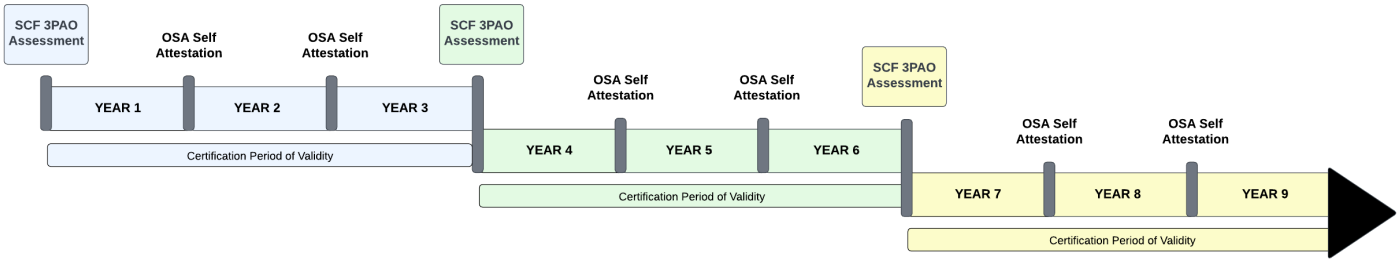
SCF CAP Certification Lifecycle

Throughout the lifecycle of the **SCF Certified™ - HIPAA Security Rule** certification, it is the responsibility of the OSA to ensure applicable controls are implemented and governed to maintain conformity.

The lifecycle of a **SCF Certified™ - HIPAA Security Rule** certification is three (3) years:

- During the first year (**Year 1**) of being certified:
  - The date of the Report on Conformity (ROC) indicates the starting date of the OSA's certification lifecycle.
  - The OSA is required to perform ongoing due care activities to maintain conformity (e.g., ongoing maintenance, change management, managing compliance requirements, etc.).
- During the second year (**Year 2**) of being certified:
  - The OSA is required to perform ongoing due care activities to maintain conformity.
  - No later than the first anniversary of the date of the ROC, the OSA it required to perform an internal assessment and provide a self-attestation that the OSA continues to conform with applicable controls.
- During the third year (**Year 3**) of being certified:
  - The OSA is required to perform ongoing due care activities to maintain conformity.
  - No later than the second anniversary of the date of the ROC, the OSA it required to perform an internal assessment and provide a self-attestation that the OSA continues to conform with applicable controls.
- At the end of the third year (**Year 3**) of being certified:
  - Original **SCF Certified™ - HIPAA Security Rule** certification expires.
  - A new third-party assessment by a SCF 3PAO is required to issue a new **SCF Certified™ - HIPAA Security Rule** certification.

This multi-year lifecycle process can be visualized below:



SCF CAP Control Designations

At the control-level, SCF Assessors must designate a status to assessed controls as follows:

(1) There are four (4) possible designations:
   a. Satisfactory;
   b. Deficient;
   c. Compensating Control; or
   d. Not Applicable (N/A);

(2) For a SCF control to be designated as Satisfactory, each of the control's applicable AOs must be designated as:
   a. Satisfactory;
   b. Compensating Control; or
   c. N/A; and

(3) If all of the following conditions exist, a SCF control designated as Deficient may be re-evaluated during the course of the assessment and for up to ten (10) business days following the active assessment period:
   a. Additional evidence:

i. Is available to demonstrate the control is satisfied; and
ii. Cannot change, or limit the effectiveness of, other requirements that have previously been scored Satisfactory; and

b. The Report on Conformity (ROC) has not been delivered to the OSA.

SCF Council Guidance: In the context of control designations, this is addressed in Standard 6 of the Cybersecurity & Data Protection Assessment Standards (CDPAS). [30]

SATISFACTORY

Satisfactory is positive, where all applicable AOs are designated as:

- Satisfied;
- N/A; or
- An compensating control is validated as being:
  - Applicable;
  - Reasonable; and
  - Implemented and operating properly.

DEFICIENT

Deficient is negative, where one (1), or more, applicable AOs are designated as:

- Deficient; or
- An compensating control cannot be validated as being:
  - Applicable;
  - Reasonable; and
  - Implemented and operating properly.

COMPENSATING CONTROL

Compensating Control is neutral, where:

- Another control, or controls, is/are designated as sufficiently reducing the risk(s) associated with the control; and
- The compensating control(s) is/are validated as being:
  - Applicable;
  - Reasonable; and
  - Implemented and operating properly.

NOT APPLICABLE (N/A)

N/A is neutral, where the control, or AO, does not apply.

SCF CAP ASSESSMENT CONFORMITY DESIGNATION

At the assessment boundary-level, SCF 3PAOs will produce a written Report on Conformity (ROC) that leverages reasonable evidence to defend the assessment conformity designation. Only one (1) of the following four (4) possible conformity designations may be used:

(1) Strictly Conforms;
(2) Conforms;
(3) Significant Deficiency; or
(4) Material Weakness.

From a pass/fail perspective, conformity designations can be viewed as:

- Passing conformity designations include:
  - Strictly Conforms; and
  - Conforms.
- Failing conformity designations include:
  - Significant Deficiency; and
  - Material Weakness.

[30] *SCF CDPAS – https://content.securecontrolsframework.com/pdf/cdpas.pdf*

SCF Council Guidance: In the context of conformity designations, this is addressed in Standard 8 of the CDPAS. [31]

STRICTLY CONFORMS

The designation of Strictly Conforms is a **positive outcome** and indicates the OSA can demonstrate Strict Conformity with its selected cybersecurity and/or data privacy controls, where one hundred percent (100%) of the assessed controls have reasonable evidence to conclude:

(1) The controls are met and operational;
(2) Any control designated as Not Applicable (N/A) is validated as such by the SCF Assessor; and/or
(3) Where applicable, compensating controls are validated by the SCF Assessor as being:
    a. Applicable;
    b. Reasonable; and
    c. Implemented and operating properly; and
(4) Assessed controls provide reasonable assurance that the OSA's security, compliance and resilience program provides adequate security, where it:
    a. Adheres to a defined and documented risk tolerance;
    b. Mitigates material cybersecurity and/or data privacy risks;
    c. Is designed to detect and protect against material cybersecurity and/or data privacy threats; and
    d. Is prepared to respond to material incidents.

CONFORMS

The designation of Conforms is a **positive outcome** and indicates the OSA can demonstrate conformity with its selected cybersecurity and/or data privacy controls, where at least eighty percent (80%) of the assessed controls have reasonable evidence to conclude:

(1) The controls are met and operational;
(2) Any control designated as N/A is validated as such by the SCF Assessor; and/or
(3) Where applicable, compensating controls are validated by the SCF Assessor as being:
    a. Applicable;
    b. Reasonable; and
    c. Implemented and operating properly;
(4) Any assessed control deficiency is not material to the OSA's security, compliance and resilience program; and
(5) Assessed controls provide reasonable assurance that the OSA's security, compliance and resilience program provides adequate security, where it:
    a. Adheres to a defined and documented risk tolerance;
    b. Mitigates material cybersecurity and/or data privacy risks;
    c. Is designed to detect and protect against material cybersecurity and/or data privacy threats; and
    d. Is prepared to respond to material incidents.

SIGNIFICANT DEFICIENCY

The designation of Significant Deficiency is a **negative outcome** and indicates the OSA can demonstrate limited conformity with its selected cybersecurity and/or data privacy controls due to a systemic problem within the OSA's security, compliance and resilience program, where:

(1) At least seventy percent (70%), but less than eighty percent (80%), of the assessed controls have reasonable evidence to conclude:
    a. The controls are met and operational;
    b. Any control designated as N/A is validated as such by the SCF Assessor; and/or
    c. Where applicable, compensating controls are validated by the SCF Assessor as being:
        i. Applicable;
        ii. Reasonable; and
        iii. Implemented and operating properly;
(2) Any assessed control deficiency is not material to the OSA's security, compliance and resilience program;
(3) Assessed controls do not provide reasonable assurance that the OSA's security, compliance and resilience program provides adequate security, where it:
    a. Adheres to a defined and documented risk tolerance;

[31] *SCF CDPAS – https://content.securecontrolsframework.com/pdf/cdpas.pdf*

b. Mitigates material cybersecurity and/or data privacy risks;
c. Is designed to detect and protect against material cybersecurity and/or data privacy threats; and
d. Is prepared to respond to material incidents; and

(4) The OSA's security, compliance and resilience program:
a. Has systemic problems inherent in the overall function of a team, department, project, application, service and/or vendor rather than a specific, isolated factor; and
b. Requires implementing limited changes to personnel, technology and/or practices to correct the design and implementation of deficient cybersecurity and/or data privacy controls.

Material Weakness

The designation of Material Weakness is a **negative outcome** and indicates where the OSA cannot demonstrate conformity with its selected cybersecurity and/or data privacy controls due to deficiencies that make it probable that reasonably expected threats will not be promptly detected or prevented, where:

(1) One (1), or more, material controls is/are deficient;
(2) Less than seventy percent (70%) of the assessed controls have reasonable evidence to conclude:
a. The controls are met and operational;
b. Any control designated as N/A is validated by the SCF Assessor and confirmed as such; and/or
c. Where applicable, compensating controls are validated by the SCF Assessor as being:
i. Applicable;
ii. Reasonable; and
iii. Implemented and operating properly;
(3) Assessed controls do not provide reasonable assurance that the OSA's security, compliance and resilience program adequately:
a. Adheres to a defined and documented risk tolerance;
b. Mitigates material cybersecurity and/or data privacy risks; and/or
c. Possesses the capability to:
i. Detect and protect against material cybersecurity and/or data privacy threats; and/or
ii. Respond to material incidents; and
(4) The OSA's security, compliance and resilience program:
a. Cannot perform its stated mission; and
b. Necessitates drastic changes to people, processes and/or technologies to remediate the deficiencies.

* See Annex 2 for a listing material controls.

SCF CAP Assessment Methods

SCF 3PAOs must use the assessment methods and criteria as defined in this section to conduct a **SCF Certified™ - HIPAA Security Rule** conformity assessment. SCF Assessors will review artifacts and other evidence to independently verify that an OSA meets the Assessment Objectives (AOs) for all applicable controls.

From an assessment perspective, the SCF provides numerous components to assist in an assessment:

- An Evidence Request List (ERL) that identifies appropriate, control-specific artifacts for SCF Assessors to examine;
- AOs to define criteria that must be met to reasonably satisfy a control objective; and
- A Secure, Compliant & Resilient Capability Maturity Model (SCR-CMM) that contains Maturity Level Criteria (MLC) to identify possible processes and/or technologies to test.[32]

SCF Assessors must perform the assessment according to the assessment method specified in the Statement of Work (SOW). SCF 3PAO must specify one (1) of the three (3) following assessment rigors:

The SCF 3PAO must specify one (1) of the three (3) following assessment methods:

(1) Manual Point In Time (MPIT);
(2) Automated Point In Time (APIT); or
(3) Automated Evidence with Human Review (AEHR).

[32] *SCR-CMM - https://content.securecontrolsframework.com/pdf/scf-capability-maturity-model.pdf*

SCF Council Guidance: APIT and AEHR may leverage Artificial Intelligence and/or Machine Learning (AI/ML) technologies. In the case of AI/ML being used, SCF 3PAOs must be prepared to demonstrate sufficient evidence of due diligence and due care to justify the integrity of the findings and overall assessment results (e.g., evidence of validating results, test cases, etc.).

MANUAL POINT IN TIME (MPIT)

MPIT is a traditional assessment methodology that:

- Is relevant to a specific point in time (time at which the controls were evaluated); and
- Relies on the manual review of artifacts to derive a finding.

AUTOMATED POINT IN TIME (APIT)

APIT utilizes automation to augment a traditional assessment methodology, where Artificial Intelligence and Autonomous Technologies (AAT) are used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

- Is relevant to a specific point in time (time at which the controls were evaluated);
- In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
- The combined output of automated and manual reviews of artifacts is used to derive a finding.

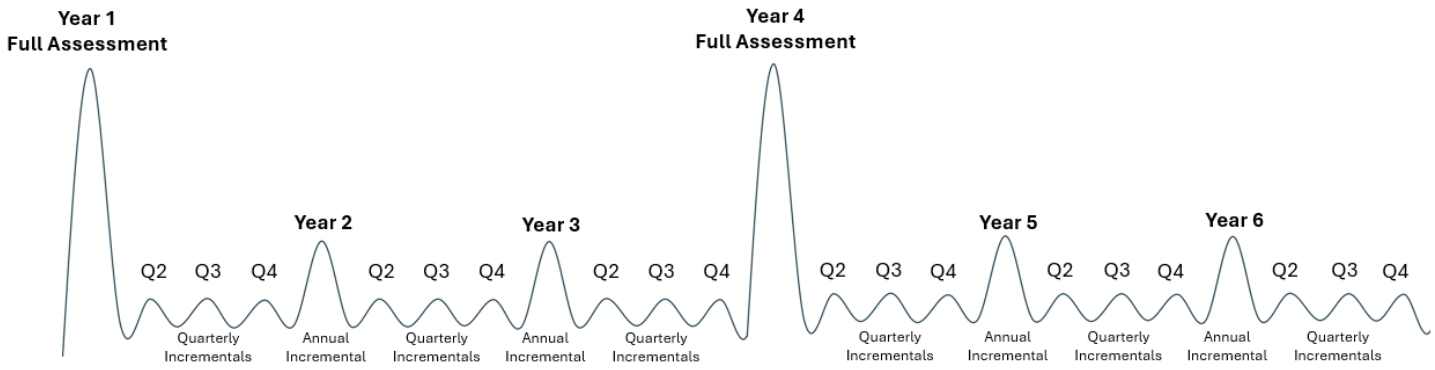
AUTOMATED EVIDENCE WITH HUMAN REVIEW (AEHR)

AEHR is used for ongoing, continuous control assessments:

- AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
- Recurring human reviews:
  - Evaluate the legitimacy of the results from automated control assessments; and
  - Validate the automated evidence review process to derive a finding.

SCF Council Guidance: The concept of "continuous compliance" is a misnomer, where it is disingenuous and falsely based on the assumption that automation without human oversight provides assurance of conformity. While it is possible to automatically pull and assess configurations against defined baselines, monitor system performance, and/or demonstrate adherence to certain technical requirements, those instances generate evidence and do not demonstrate conformity on a broader scale (e.g., breadth of a comprehensive audit / assessment). Based on the cadence of these automated checks, existing technologies support an "incremental" approach than a "continuous" approach to conformity demonstration.

The SCF CAP leverages the AEHR assessment methodology as a Continuous Incremental Conformity Assessment (CICA). This incremental approach is depicted in the graphic below, where smaller, recurring assessments augment periodic, full assessments to provide assurance beyond a single point-in-time:



Similar to how controls have different relative weights from a risk perspective, not every control changes at the same cadence, so OSAs need to define a Conformity Validation Cadence (CVC) for each control. This value signifies the cadence that the output of a control should be checked, not how often the control activity is performed. Understanding the CVC helps an OSA understand which controls are dynamic (e.g., near real-time, daily, weekly or month) and which controls are relatively static (e.g., quarterly, semi-annual or annual changes). This understanding of its control environment can help an OSA develop an optimal approach to oversee its security, compliance and resilience efforts.

The assumption is that upon the tri-annual SCF CAP assessment, those automated controls will require minimal scrutiny, based on the historical evidence of conformity during the certification period. This is intended to reduce the associated financial and labor burden of the tri-annual SCF CAP assessment to re-establish the conformity baseline.

Specific to the SCF CAP:

- A full assessment (e.g., MPIT or APIT) is conducted to establish the baseline;
- The Statement of Work (SOW) between the 3PAO and OSA establishes:
  - Controls to be assessed as part of incremental reviews; and
  - Cadence of incremental assessments (e.g., monthly, quarterly or annual).
- Automated feeds are configured to generate evidence (e.g., vulnerability scans, SIEM reports, GRC tool metrics); and
- Evidence is collected to layer onto prior assessments, with older unchanged evidence remaining valid until expiration (e.g., tri-annual certification period).

SCF CAP Assessment Criteria

At a minimum:

- Standard rigor should be used for MPIT assessments;
- Enhanced rigor should be used for APIT assessments; and
- Comprehensive rigor should be used for AEHR assessments.

SCF Assessors must perform the assessment at a level of rigor specified in the Statement of Work (SOW). SCF 3PAO must specify one (1) of the three (3) following assessment rigors:

(1) Level 1: STANDARD;
(2) Level 2: ENHANCED; or
(3) Level 3: COMPREHENSIVE.

See Appendix B: Assessment Rigor for more details on this subject.

Level 1 Rigor: Standard

Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:

- Implemented; and
- Free of obvious errors.

Level 2 Rigor: Enhanced

Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:

- The applicable controls are:
  - Implemented; and
  - Free of obvious/apparent errors; and
- There are increased grounds for confidence that the applicable controls are:
  - Implemented correctly; and
  - Operating as intended.

Level 3 Rigor: Comprehensive

Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:

- Whether the applicable controls are:
- Implemented; and
- Free of obvious/apparent errors;
- Whether there are further increased grounds for confidence that the applicable controls are:
- Implemented correctly; and
- Operating as intended on an ongoing and consistent basis; and
- There is support for continuous improvement in the effectiveness of the applicable controls.

THIRD-PARTY ASSESSMENT, ATTESTATION AND CERTIFICATION (3PAAC) STANDARDS

The SCF Third-Party Assessment, Attestation and Certification Assessment Guide Standards (SCF 3PAAC AGS) are based on the Cybersecurity & Data Protection Assessment Standards (CDPAS).[33]

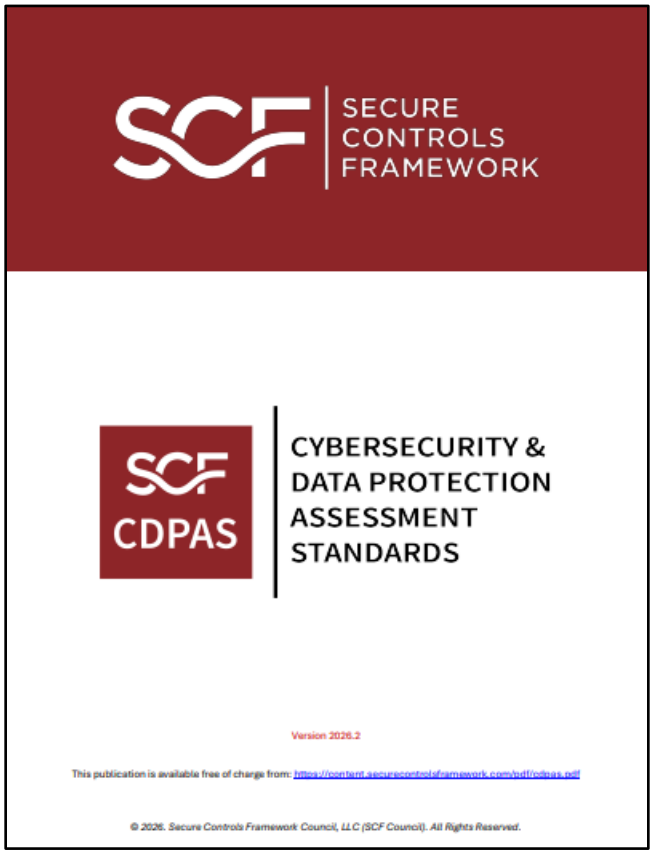
The CDPAS provides an industry standard, where exceptions by either OSA or SCF 3PAOs must be justified. If additional clarification is required, the CDPAS provides additional context for the standards in the form of justifications and guidelines.

The CDPAS apply to:

- OSAs;
- SCF Assessors; and
- SCF 3PAOs.

SCF Council Guidance: It is imperative for OSA personnel and SCF Assessors to be familiar with the current standards established by the CDPAS, since that governs the SCF CAP assessment process. This is a free standard that is available to all stakeholders.

From an audit and quality assurance perspective, the SCF Council will evaluate based on the current version of the CDPAS.



[33] SCF CDPAS – https://content.securecontrolsframework.com/pdf/cdpas.pdf

AUTHORITATIVE MAPPINGS FOR PERFORMING CONFORMITY ASSESSMENTS

To perform a conformity assessment, the assessment methodology requires:

- Authoritative mappings;
- Reasonable granularity to address the intent of the control; and
- Objective criteria to determine if the control is adequately:
  - Designed;
  - Implemented; and
  - Operating as intended.

The SCF CAP addresses these requirements through:

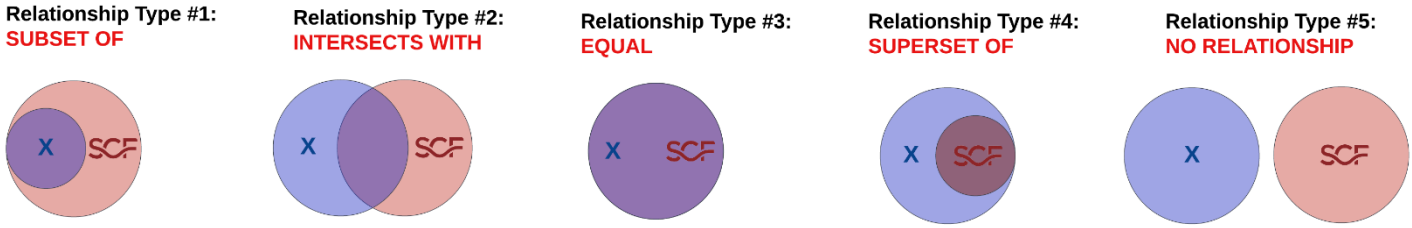
- Granular controls mapped according to NIST IR 8477 Set Theory Relationship Mapping (STRM) guidelines;[34]
- Control weighting to determine material controls;
- An Evidence Request List (ERL) to determine a reasonable set of artifacts;
- Maturity criteria to provide reasonable expectations for implemented capabilities; and
- Assessment Objectives (AOs) that an SCF Assessor can leverage to analyze control design, implementation and operation.

NIST IR 8477 - BASED SET THEORY RELATIONSHIP MAPPING (STRM)

The SCF leverages NIST IR 8477 STRM guidelines for crosswalk mapping, since STRM is generally well-suited to evaluate cybersecurity and data privacy laws, regulations and frameworks. NIST IR 8477 is the US Government's playbook for how to perform crosswalk mapping between different cybersecurity and data privacy laws, regulations and frameworks.

STRM is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., security, compliance and resilience requirements). Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two (2) distinct concepts:

(1) Subset Of;
(2) Intersects With;
(3) Equal;
(4) Superset Of; and
(5) No Relationship.



Specific to STRM terminology:

- **Reference Document** – This will always be the SCF. The Reference Document is being mapped to the Focal Document.
- **Focal Document** – This will always be the law, regulation or framework is the source document that is being mapped from (e.g., HIPAA Security Rule).
- **Focal Document Element (FDE)** – This is the granular requirement/control from the Focal Document to is being mapped to.

STRM also allows the strength of the mapping to be captured, where STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two (2) concepts are related:

(1) Syntactic: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.

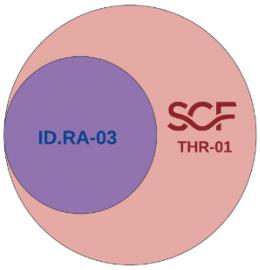
[34] *NIST IR 8477 - https://csrc.nist.gov/pubs/ir/8477/final*

(2) Semantic: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
(3) Functional: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

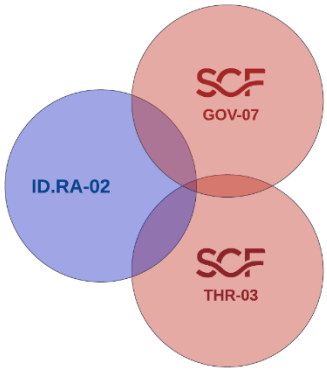
SCF Council Guidance: SCF mappings leverage only the Functional context justification for STRM, since the mappings focus on results of control execution.

The use of STRM enables the SCF to create "backwards mapping" from HIPAA Security Rule to SCF controls that are justifiable, based on relationship types and the rationale used to perform the mapping. Graphical examples for STRM relationships are shown below:

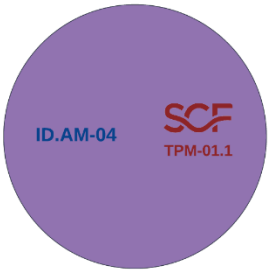
Relationship Type: SUBSET OF



Relationship Type: INTERSECTS WITH



Relationship Type: EQUAL



These STRM graphics can be downloaded from the SCF website.[35]

APPLICABLE SCF STRM VERSION

As the applicable STRM for a law, regulation or framework is released/updated, a new version of the SCF STRM will be generated. Therefore, the most current version of the SCF are expected be used for SCF CAP purposes.

When a new version of STRM is published for a law, regulation or framework, the previous version of that STRM is deprecated one hundred eighty (180) days after the release of the new version.

[35] *SCF STRM - https://content.securecontrolsframework.com/pdf/scf-set-theory-relationship-mapping.pdf*

NIST CYBERSECURITY FRAMEWORK 2.0 CONTROLS

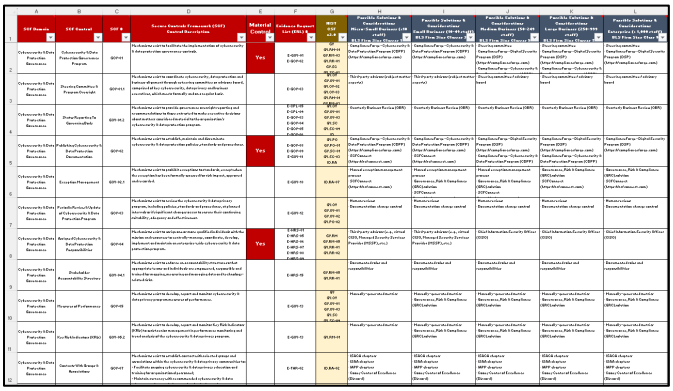
The SCF CAP provides two (2) formats of mappings:

1. Set Theory Relationship Mapping (STRM) formatted HIPAA Security Rule to SCF; and
2. SCF to HIPAA Security Rule (traditional SCF mappings).

STRM is used to justify the mappings leveraged by the SCF for HIPAA Security Rule.

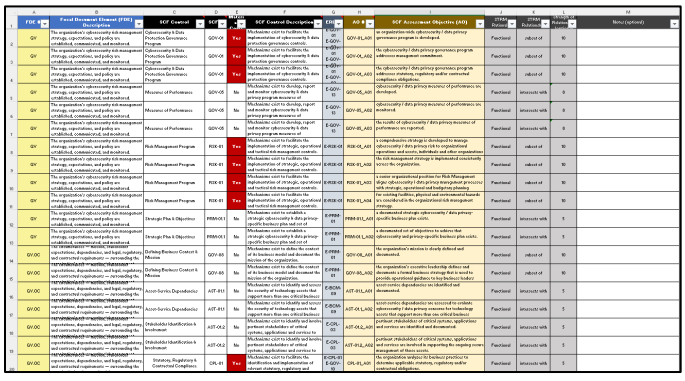
STRM - HIPAA SECURITY RULE TO SCF MAPPINGS

Annex 1 to the HIPAA Security Rule Assessment Guide contains the STRM view of crosswalk mapping from HIPAA Security Rule to SCF controls.



SCF TO HIPAA SECURITY RULE MAPPINGS

Annex 2 to the HIPAA Security Rule Assessment Guide contains crosswalk mapping from SCF to HIPAA Security Rule controls (traditional SCF crosswalk formatting).



SCF Council Guidance: The most efficient method of addressing HIPAA Security Rule controls is through the format provided in Annex 2. The reason for this is it provides a significant reduction in duplication from one-to-many mapping relationships (e.g., SCF controls that address multiple HIPAA Security Rule requirements).

ERRATA

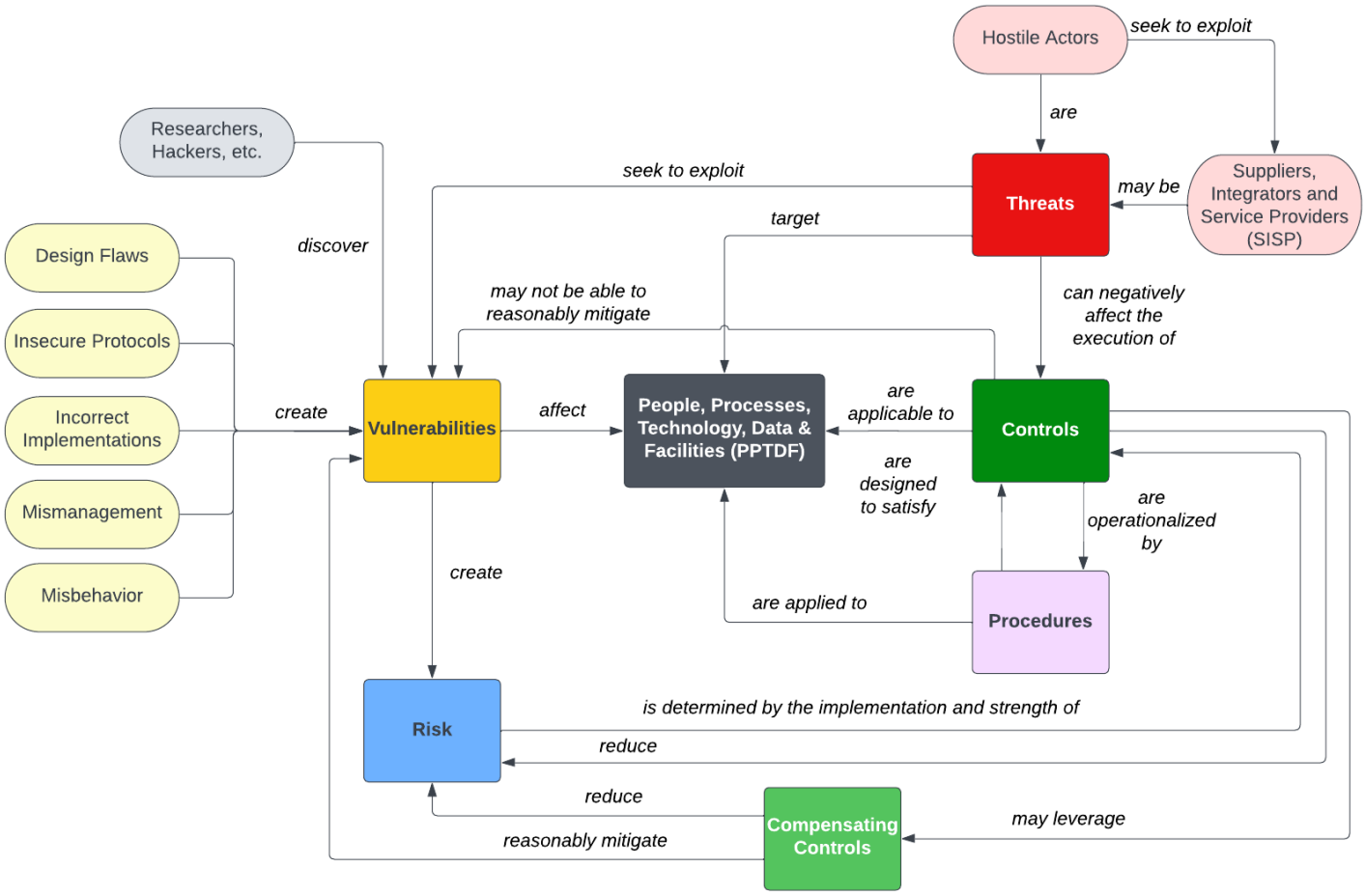
Version 1.3 (March 2026) includes:

(1) Streamlined the document to reference the CDPAS, instead of duplicating content in the assessment guide.
(2) Added “SCF Council Guidance” callouts.
(3) Updated URLs.

APPENDICES

APPENDIX A: RISK TERMINOLOGY NORMALIZATION

Threat, vulnerability and risk management practices are meant to achieve a minimum level of protection - this equates to a reduction in the total risk due to the protections offered by implemented controls. These ecosystem components have unique meanings that need to be understood to reasonably protect people, processes, technology and data. Understanding the context of how these components integrate can lead to more meaningful and practical risk management practices.



As it pertains to the CDPAS:

- Risk Appetite: *the types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.*[36]
- Risk Tolerance: *the level of risk an entity is willing to assume in order to achieve a potential desired result.*[37]
- Risk Threshold: *values used to establish concrete decision points and operational control limits to trigger management action and response escalation.*[38]

RISK APPETITE

A risk appetite is a broad "risk management concept" used to inform employees about what is and is not acceptable, regarding risk management from an organization's executive leadership team. A risk appetite does not contain granular risk management criteria and is primarily a "management statement" that is subjective. Similar in concept to how a policy is a *"high-level*

[36] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*
[37] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*
[38] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*

statement of management intent," an organization's defined risk appetite is a high-level statement of how all, or certain types of, risk are willing to be accepted. [39]

Examples of an organization stating its risk appetite from basic to more complex statements:

- *"[organization name] is a low-risk organization and will avoid any activities that could harm its customers."*
- *"[organization name] will aggressively pursue innovative solutions through Research & Development (R&D) to provide industry-leading products and services to our clients, while maintaining a Moderate Risk Appetite. Developing breakthrough products and services does invite potential risk through changes to traditional supply chains, disruptions to business operations and changing client demand. Proposed business practices that pose greater than a Moderate Risk will be considered on a case-by-case basis for financial, operational and legal implications."*

It is important to point out that in many immature risk programs, risk appetite statements are divorced from reality. Executive leaders mean well when they issue risk appetite statements, but the Business As Usual (BAU) practices routinely violate the risk appetite. This is often due to numerous reasons that include, but are not limited to:

- Technical debt;
- Dysfunctional management decisions;
- Insecure practices;
- Inadequate funding/resourcing;
- Improperly scoped support contracts (e.g., Managed Service Providers (MSPs), consultants, vendors, etc.); and
- Lack of pre-production security testing.

Risk Tolerance

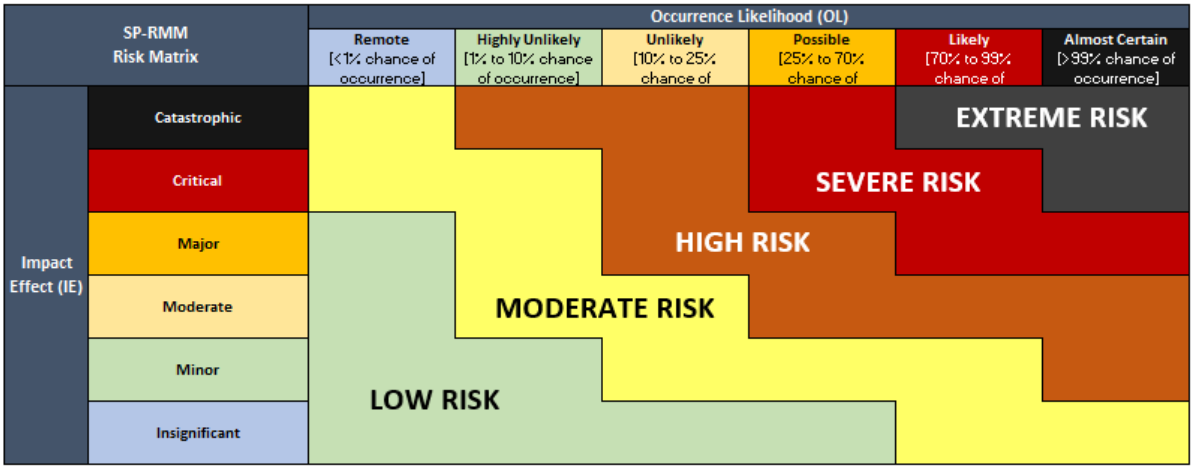
Risk tolerance is based on objective criteria, unlike the subjective, conceptual nature of a risk appetite. Defining objective criteria is a necessary step to categorize risk on a graduated scale. Establishing objective criteria to quantify the impact of risk enables risk assessments to leverage those same criteria and assist decision-makers in their risk management decisions (e.g., accept, mitigate, transfer or avoid).

From a graduated scale perspective, it is possible to define "tolerable" risk criteria to create five (5) useful categories of risk:

(1) Low Risk;
(2) Moderate Risk;
(3) High Risk;
(4) Severe Risk; and
(5) Extreme Risk.

There are two (2) objective criteria that go into defining what constitutes a low, moderate, high, severe or Extreme Risk includes:

(1) Impact Effect (IE); and
(2) Occurrence Likelihood (OL).



[39] *ComplianceForge Hierarchical Cybersecurity Governance Framework (HCGF) - https://content.complianceforge.com/Hierarchical-Cybersecurity-Governance-Framework.pdf*

The six (6) categories of IE are:

(1) Insignificant *(e.g., organization-defined little-to-no impact to business operations);*
(2) Minor *(e.g., organization-defined minor impacts to business operations)*;
(3) Moderate *(e.g., organization-defined moderate impacts to business operations)*;
(4) Major *(e.g., organization-defined major impacts to business operations)*;
(5) Critical *(e.g., organization-defined critical impacts to business operations)*; and
(6) Catastrophic *(e.g., organization-defined catastrophic impacts to business operations)*.

The six (6) categories of OL are:

(1) Remote possibility *(e.g., <1% chance of occurrence)*;
(2) Highly unlikely *(e.g., from 1% to 10% chance of occurrence)*;
(3) Unlikely *(e.g., from 10% to 25% chance of occurrence)*;
(4) Possible *(e.g., from 25% to 70% chance of occurrence)*;
(5) Likely *(e.g., from 70% to 99% chance of occurrence)*; and
(6) Almost certain *(e.g., >99% chance of occurrence)*.

There are three (3) general approaches commonly employed to estimate OL:

(1) Relevant historical data;
(2) Probability forecasts; and
(3) Expert opinion.

An organization's risk tolerance is influenced by several factors that includes, but is 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.
- Executive management decisions.

Low Risk Tolerance

Organizations that may adopt a Low Risk Tolerance include, but are not limited to, those that:

- Provide products and/or services that are necessary for the population to maintain normalcy in daily life;
- Exist in a highly regulated industry with explicit cybersecurity and/or data protection requirements;
- Store, process and/or transmit highly sensitive/regulated data;
- May be a legitimate target 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 and data protection 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 liability 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 Risk Tolerance

Organizations that may adopt a Moderate Risk Tolerance include, but are not limited to, those that:

- Exist in a regulated industry that has specific cybersecurity and/or data protection requirements (e.g., CMMC, PCI DSS, SOX, GLBA, RMF, etc.);
- Store, process and/or transmit sensitive/regulated data;
- Have "flow down" requirements from customers that require adherence to certain cybersecurity and/or data protection requirements;
- Have executive management support for initiatives to secure sensitive / regulated data enclaves;
- May be a legitimate target for attackers who wish to financially benefit from stolen information or ransom; and
- Have cyber-related liability 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 (MSSPs), etc.);
- Manufacturing (high value);
- Healthcare;
- Defense Industrial Base (DIB) contractors and subcontractors;
- Legal services (e.g., law firms); and
- Construction (high value).

High Risk Tolerance

Organizations that may adopt a High Risk Tolerance include, but are not limited to, those that:

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

Organizations that may choose to operate with a High Risk Tolerance include, but are not limited to:

- Startups;
- Hospitality industry (e.g., restaurants, hotels, etc.);
- Construction;
- Manufacturing; and
- Personal services.

Severe Risk Tolerance

Organizations that may adopt a Severe Risk Tolerance include, but are not limited to, those that:

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

Organizations that may choose to operate with a Severe Risk Tolerance include, but are not limited to:

- Startups; and
- Artificial Intelligence (AI) developers.

Extreme Risk Tolerance

Organizations that may adopt an Extreme Risk Tolerance include, but are not limited to, those that:

- Exist in an unregulated industry, pertaining to expected cybersecurity and/or data protection practices;
- Do not store, process and/or transmit sensitive/regulated data;
- Lack management support for cybersecurity and data protection governance practices; and

- Do not have cyber-related liability insurance.

Organizations that may choose to operate with an Extreme Risk Tolerance include, but are not limited to:

- Startups; and
- AI developers.

RISK THRESHOLDS

Risk thresholds are directly tied to risk tolerance and utilize organization-specific criteria (e.g., acceptable and unacceptable parameters). These risk thresholds exist between the different levels of risk tolerance (e.g., Low, Moderate and High Risk). By establishing these risk thresholds, it provides a means of comparing relative risk to an organization. Risk thresholds are criteria that are unique to an organization such as organization-specific activities / scenarios that could:

- Damage the organization's reputation;
- Negatively affect short-term and long-term profitability; and/or
- Impede business operations.

Risk thresholds are entirely unique to each organization, based on several factors that include:

- Financial stability;
- Management preferences;
- Compliance obligations (e.g., statutory, regulatory and/or contractual); and
- Insurance coverage limits.

APPENDIX B: ASSESSMENT RIGOR

The SCF CAP assessment rigor is based on assessment methods described in NIST SP 800-172A Appendix C.[40] There are three (3) levels of rigor:

(1) Standard;
(2) Enhanced; and
(3) Comprehensive.

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.

LEVEL 1 RIGOR: STANDARD

Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:

(1) Implemented; and
(2) Free of obvious errors.

Standard rigor represents sufficient due care in the evaluation of cybersecurity and/or data protection controls. Standard rigor is appropriate for the Manual Point In Time (MPIT) assessment methodology that:

(1) Is relevant to a specific point in time (time at which the controls were evaluated); and
(2) Relies on the manual review of artifacts to derive a finding.

<table>
<tr><th colspan="2">STANDARD
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
Security safeguard existence;
Functionality;
Correctness;
Completeness; and
Potential for improvement over time.
Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:
(1) Implemented; and
(2) Free of obvious errors.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>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</td><td>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</td><td>A test methodology assumes no knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as “black box” testing.</td></tr>
</table>

[40] *NIST SP 800-172A - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172A.pdf*

		body of evidence or documentation including: ▪ Functional-level descriptions for mechanisms; ▪ High-level process descriptions for activities; and ▪ Documents for specifications.	generalized, high-level questions.	This type of testing is conducted using: ▪ A functional specification for mechanisms; and A high-level process description for activities.
Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task	N/A

			execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	

LEVEL 2 RIGOR: ENHANCED

Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:

(1) The applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors; and
(2) There are increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended.

Enhanced rigor is appropriate for the Automated Point In Time (APIT) assessment methodology that utilizes automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

(1) Is relevant to a specific point in time (time at which the controls were evaluated);
(2) In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
(3) The combined output of automated and manual reviews of artifacts is used to derive a finding.

<table>
<tr><th colspan="2">ENHANCED
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
Security safeguard existence;
Functionality;
Correctness;
Completeness; and
Potential for improvement over time.
Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:
(1) The applicable controls are:
a. Implemented; and
b. Free of obvious/apparent errors; and
(2) There are increased grounds for confidence that the applicable controls are:
a. Implemented correctly; and
b. Operating as intended.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>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</td><td>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.</td><td>A test methodology assumes some knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as “gray box” testing.

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-</td></tr>
</table>

		information for mechanisms; ▪ High-level process descriptions and implementation procedures for activities; and ▪ Documents and related documents for specifications.		level process description; and ▪ A high-level description of integration into the operational environment for activities.
Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task	N/A

			execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	

LEVEL 3 RIGOR: COMPREHENSIVE

Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:

(1) Whether the applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors;
(2) Whether there are further increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended on an ongoing and consistent basis; and
(3) There is support for continuous improvement in the effectiveness of the applicable controls.

Comprehensive rigor is appropriate for the Automated Evidence with Human Review (AEHR) assessment methodology that is used for ongoing, continuous control assessments:

(1) AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
(2) Recurring human reviews:
    a. Evaluate the legitimacy of the results from automated control assessments; and
    b. Validate the automated evidence review process to derive a finding.

<table>
<tr><th colspan="2">COMPREHENSIVE
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
Security safeguard existence;
Functionality;
Correctness;
Completeness; and
Potential for improvement over time.
Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:
(1) Whether the applicable controls are:
a. Implemented; and
b. Free of obvious/apparent errors;
(2) Whether there are further increased grounds for confidence that the applicable controls are:
a. Implemented correctly; and
b. Operating as intended on an ongoing and consistent basis; and
(3) There is support for continuous improvement in the effectiveness of the applicable controls.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>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</td><td>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:</td><td>Test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as “white box” testing.</td></tr>
</table>

		body of evidence or documentation including:
		▪ 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.
			▪ 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.
				This type of testing is conducted using:
				▪ A functional specification;
				▪ Extensive system architectural information (e.g., high-level design, low-level design);
				▪ Implementation representation (e.g., source code, schematics) for mechanisms;
				▪ A high-level process description; and
				▪ A detailed description of integration into the operational environment for activities.

	Breadth of Coverage	Examinations 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 applicable controls are:
		  ○ Implemented; and
		  ○ Free of obvious/apparent errors;
		▪ Whether there are further increased grounds for confidence that the applicable controls are:
		  ○ Implemented correctly; and
		  ○ Operating as intended on an ongoing and consistent basis; and
		▪ There is support for continuous improvement in the effectiveness of the applicable controls.
			Interviews use 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 applicable controls are:
			  ○ Implemented; and
			  ○ Free of obvious/apparent errors;
			▪ Whether there are further increased grounds for confidence that the applicable controls are:
			  ○ Implemented correctly; and
			  ○ Operating as intended on an ongoing and consistent basis; and
			▪ There is support for continuous improvement in the effectiveness of the applicable controls.
				Testing 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 applicable controls are:
				  ○ Implemented; and
				  ○ Free of obvious/apparent errors;
				▪ Whether there are further increased grounds for confidence that the applicable controls are:
				  ○ Implemented correctly; and
				  ○ Operating as intended on an ongoing and consistent basis; and
				▪ There is support for continuous improvement in the effectiveness of the applicable controls.

Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.

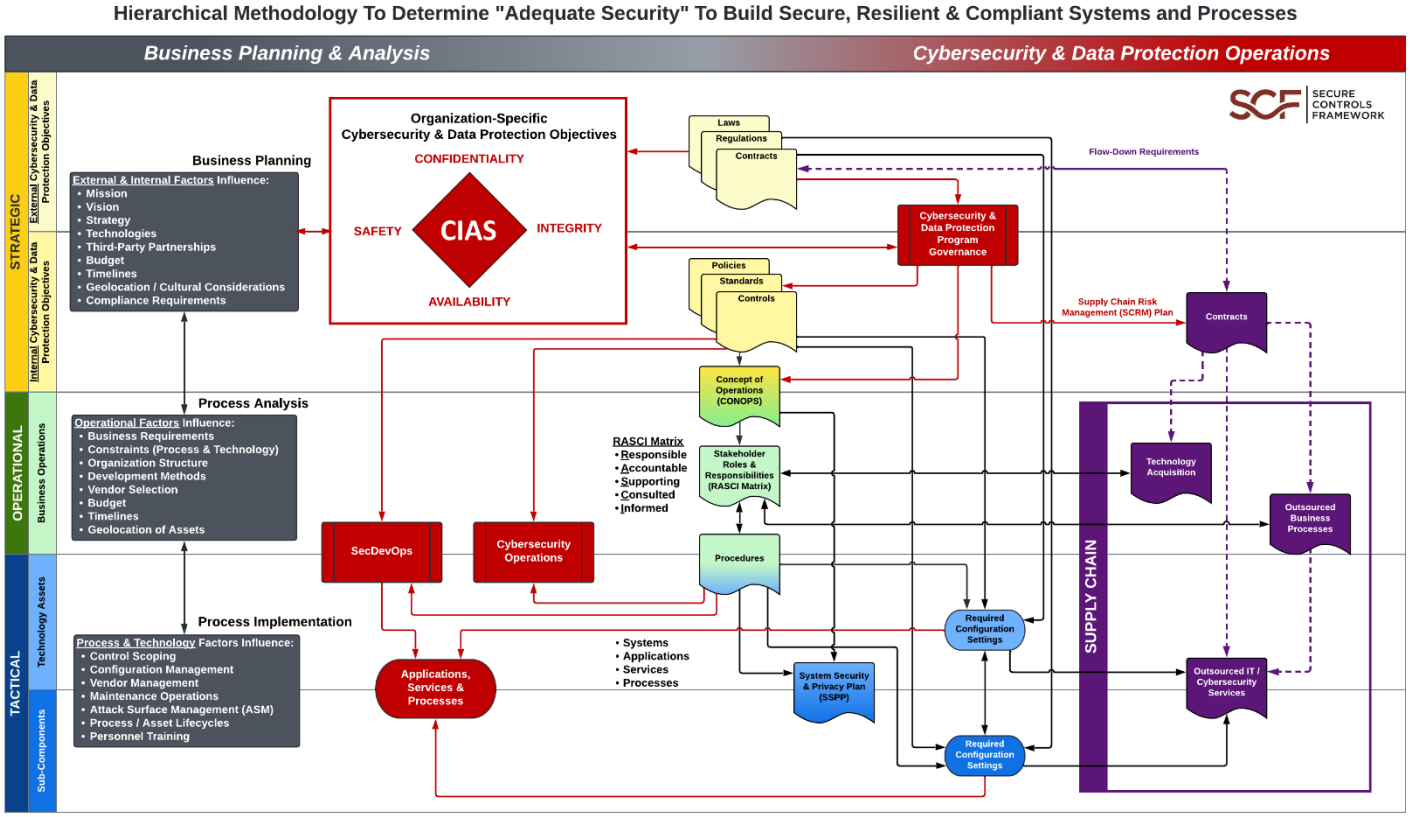
		▪ Firmware.		
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	N/A

APPENDIX C: ADEQUATE SECURITY

The SCF CAP recognizes that no technology can provide "absolute security" due to the limits of human certainty. This uncertainty exists in the lifecycle of every system, application and/or product and is often due to the constraints of cost, schedule, performance, feasibility and practicality. Therefore, trade-offs must 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. [41]

The SCF CAP, through the CDPAS, leverages concepts from NIST SP 800-160 to explain the holistic concepts of how broader business planning and analysis ultimately lead to actionable cybersecurity and/or data protection requirements. Understanding this hierarchical nature of requirements is a fundamental construct of cybersecurity and/or data protection control governance processes.

This concept is depicted in the following graphic for how the concept of adequate security is based on business planning and analysis as it relates to establishing protection requirements:[42]



An organization publishes policies to eliminate potential gaps in that desired governed behavior to achieve "adequate security" 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 accomplish the organization's mission and overall strategy.

An organization's policies ultimately define the behavior of Individual Contributors (IC) (e.g., engineers, analysts, developers, etc.) 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 implementing organizational security policies.

[41] *NIST SP 800-160 Vol 1 Rev 1 Appendix C*
[42] *SCF Adequate Security Determination Process - https://securecontrolsframework.com/content/adequate-cybersecurity-methodology.pdf*

The required configuration settings for technology assets must include technical and business requirements, which ultimately fall under organizational cybersecurity and/or data protection policies. Requirements can be categorized as follows: [43]

- 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 in a design-dependent manner.

Establishing 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.[44] 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 degrades some other aspects of system performance or requires an unacceptable operational commitment.

Defining 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, human 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.

Defining System Security Requirements

System requirements specify the technical view of a system or solution that meets the identified 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."*[45] Since engineers/architects/developers do not design, code and maintain Applications, Services and Processes (ASP) in a vacuum, they need to embrace a "system of systems" mindset toward system interaction since there are legitimate cybersecurity and/or data protection concerns with untrustworthy dependencies. A system of systems is a *"set of systems and*

[43] *NIST SP 800-160 Vol 1 Rev 1 Appendix C*
[44] *NIST SP 800-160 Vol 1 Rev 1*
[45] *NIST SP 800-160 Vol 1 Rev 1*

system elements interacting to provide a unique capability that none of the constituent systems can accomplish on their own."[46] 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:
  - Development environments;
  - Production systems, applications and services;
  - Training systems; and
  - Maintenance systems; and
- Interoperating Systems. These interact with systems to jointly perform a function during the utilization and sustainment stages of the system life cycle. Interoperating systems often form a system of systems.

[46] *NIST SP 800-160 Vol 1 Rev 1*

ANNEXES

Download the annexes from: https://content.securecontrolsframework.com/cap/annexes-hipaa-security.xlsx

ANNEX 1: HIPAA SECURITY RULE TO SCF CROSSWALK MAPPING

Contains the Set Theory Relationship Mapping (STRM) view of crosswalk mapping from HIPAA Security Rule to SCF controls.

ANNEX 2: SCF TO HIPAA SECURITY RULE CROSSWALK MAPPING

Contains:

- Crosswalk mapping from SCF to HIPAA Security Rule controls; and
- HIPAA Security Rule-specific Maturity Level Criteria (MLC). MLC are located on columns H through M on the Annex 2 tab of the Excel spreadsheet.

SCF Council Guidance: The most efficient method of addressing HIPAA Security Rule controls is through the format provided in Annex 2. The reason for this is it provides a significant reduction in duplication (e.g., one to many mapping relationship).

ANNEX 3: HIPAA SECURITY RULE ASSESSMENT OBJECTIVES (AOS)

Contains a complete listing of SCF-based AOs for HIPAA Security Rule; and

SCF Council Guidance: AOs are located on columns E on both the "Annex 1" and "Annex 3" tabs of the Excel spreadsheet.

ANNEX 4: HIPAA SECURITY RULE EVIDENCE REQUEST LIST (ERL)

Contains a complete listing of HIPAA Security Rule-specific evidence artifacts; and

ANNEX 5: SCF CAP RASCI

Contains a RASCI matrix for 3PAAC Services; and

ANNEX 6: 3PAAC DPIA TEMPLATE

Contains a reference DPIA template that SCF 3PAOs can use to assess data protection risks as part of 3PAAC Services, if applicable.

ANNEX 7: MATERIALITY THRESHOLDS

Contains a materiality threshold calculator that an OSA can use to determine its materiality threshold.