ODA3 INSTITUTE

ADOPTION GUIDE

Mapping GAISSF™ to

SOC 2

Doc ID: ODA3-2026-08-WHP-COM-006
Classification: Public / Freely Distributable

Executive Summary

Organizations already reporting under SOC 2 often ask the same question before adopting GAISSF™: does this mean starting over? This guide answers that directly. It is not a control-by-control crosswalk — it is a structural orientation showing where SOC 2 and GAISSF™ address related concerns differently, where GAISSF™ may add control or evidence granularity, and what should be examined through a formal crosswalk.

> **METHODOLOGY NOTE**
> This guide is introductory and conceptual. It contains no client outcome data, no proprietary telemetry, and no incident statistics. It does not constitute a formal conformance mapping or certification determination. Reference baseline: AICPA Trust Services Criteria (2017), with points of focus revised in 2022. As verified on 12 August 2026, this remains the current published version; this guide should be revalidated against any superseding release.

1. Why This Comparison Matters

SOC 2 is an attestation framework, not a certification: a licensed CPA firm examines a service organization's controls against the AICPA's Trust Services Criteria (TSC) and issues a report, rather than certifying conformance to a published standard. SOC 2 examinations address controls relevant to the Trust Services Criteria; the Security category applies in every SOC 2 examination and is addressed through the Common Criteria (CC1–CC9), while Availability, Processing Integrity, Confidentiality, and Privacy may be included according to engagement scope. A Type I report addresses the suitability of control design at a specified date; a Type II report addresses suitability of design and operating effectiveness over a specified period. The TSC provides criteria against which an organization's controls are evaluated; it does not prescribe a single fixed control catalogue — organizations design controls appropriate to their systems and circumstances to address the applicable criteria. GAISSF™ uses a control-based architecture: 9 domains and a published architecture comprising 52 foundational controls, with explicit evidence expectations, designed to complement and be mapped against frameworks like SOC 2 rather than replace them.

The objective of this guide is to identify where existing attestation work may support GAISSF™ requirements, where the two frameworks address related concerns differently, and what a formal crosswalk should examine for correspondence, gaps, and potential reuse.

2. Structural Comparison

Aspect	SOC 2	GAISSF™
Structure	5 Trust Services Categories; Security applies to every examination, via CC1–CC9	9 domains, 52 foundational controls
Orientation	Criteria evaluated against organization-designed controls; no prescribed catalogue	Defined control requirements, implementation, assurance evidence
Evidence model	Type I — design suitability at a date; Type II — design suitability and operating effectiveness over a period	Explicit control-linked evidence expectations
Conformance / assurance model	CPA-issued attestation report; not certification against a standard	Defined conformance architecture; Appendix P.1 profile where appropriate

ODA3 Institute's own assessment and certification infrastructure is under development; conformance claims for GAISSF™ should be read against that status.

3. What Your SOC 2 Work May Provide → Where There Is Clear Conceptual Correspondence → Where GAISSF™ May Add Depth

What your existing SOC 2 work may provide

Existing SOC 2 work may provide a documented control environment addressing governance, risk assessment, logical and physical access, system operations, and change management (the Common Criteria), along with an auditor's report evidencing control design or operating effectiveness. The extent to which these support GAISSF™ requirements must be verified for the system and scope being examined.

Where there is clear conceptual correspondence

GAISSF™ D6 (Governance, Accountability & Human Oversight) and SOC 2's governance- and risk-oriented Common Criteria (drawing on COSO's internal-control principles) address related organizational-governance concerns. SOC 2's logical-access and system-operations criteria relate conceptually to GAISSF™'s runtime-security and access-control domains. The relationship is conceptual and does not establish one-to-one control equivalence — correspondence at the criterion-to-GAISSF-control level requires a formal crosswalk.

Where GAISSF™ may add depth

- GAISSF™ organizes model integrity, runtime security, agentic risk, and AI supply-chain security into dedicated control domains (D1–D4). SOC 2's Common Criteria are general-purpose system and organizational control criteria rather than an AI-specific control catalogue; a formal crosswalk is required to determine the degree of coverage for any specific GAISSF™ control.
- GAISSF™ links its control architecture to identifiable implementation evidence and assurance expectations specific to AI systems. SOC 2 evidence is evaluated within the attestation engagement against the applicable Trust Services Criteria and the organization's control design; it is not structured around an AI-specific control catalogue.
- Appendix P.1 SMB Quick-Start, a defined GAISSF™ conformance-profile entry point, where applicable — distinct from, and not directly equivalent to, determining which Trust Services Categories are included within a SOC 2 examination.

> **KEY PRINCIPLE**
> Assurance is demonstrated, not asserted. A control claim is only as credible as the evidence supporting its implementation and operation. GAISSF™ applies that principle through a control-and-evidence architecture that can complement an organization's existing SOC 2 attestation work.

4. Areas to Examine in a Formal Crosswalk

A formal crosswalk should examine, rather than assume, the degree to which existing SOC 2 controls and audit evidence support GAISSF™ requirements. The examination should include, where applicable: the extent to which existing evidence supports AI-specific technical requirements; model and runtime security; agentic-system controls; AI supply-chain controls; and correspondence between SOC 2 audit evidence and specific GAISSF™ requirements.

5. Recommended Next Action

- 1. Identify one AI system already within your SOC 2 audit scope.
- 2. Document which Trust Services Categories and Common Criteria apply to that system, and whether your most recent report is Type I or Type II.
- 3. Determine the appropriate GAISSF™ scope or profile independently, using GAISSF™ scoping rules.
- 4. Compare existing SOC 2 controls and audit evidence against the applicable GAISSF™ requirements.
- 5. Record supported correspondence, partial correspondence, gaps, and unknowns — rather than assuming equivalence.
- 6. Use the eventual formal GAISSF™–SOC 2 crosswalk when available.

> **NOTABLY ABSENT**
>
> This guide does not establish control equivalence, coverage percentage, conformance inheritance, regulatory equivalence, or certification credit between SOC 2 and GAISSF™. It is not a control-by-control crosswalk or formal assessment methodology. Any claimed correspondence must be verified at the applicable criterion and GAISSF™ control level. SOC 2 reports are issued by licensed CPA firms; AICPA does not itself certify organizations. A SOC 2 report does not, without independent verification, establish GAISSF™ conformance or correspondence to specific GAISSF™ controls.

The Relationship at a Glance

- SOC 2 — Trust Services Criteria evaluated by a licensed CPA firm → attestation report on suitability of control design and, where Type II, operating effectiveness.
- GAISSF™ — applicable domain/control scope → control requirements, implementation evidence, and assurance expectations.

Correspondence between the two must be established at the criterion-to-GAISSF-control level — it is tested, not declared.

Next Reading

- The 10-Minute Introduction to GAISSF™
- GAISSF™ Appendix P.1 SMB Quick-Start Guide
- Mapping GAISSF to NIST AI RMF
- Mapping GAISSF to ISO/IEC 42001