SOC 2 & NIST CSF 2.0 Alignment Guide

A Comprehensive Mapping of Trust Services Criteria to the NIST Cybersecurity Framework

Prepared by Iron City IT Advisors LLC | William Laukaitis, CEO

Executive Summary

This guide bridges the **AICPA SOC 2 Trust Services Criteria (TSC)** with the **NIST Cybersecurity Framework 2.0 (CSF)** to help organizations build unified security and compliance programs.
SOC 2 defines **what** must be controlled; NIST CSF defines **how** to structure those controls. Aligning both improves audit readiness, cross-framework efficiency, and executive visibility.

Framework Purposes

Framework	Purpose	Governing Body
SOC 2 (TSC)	Attestation of control effectiveness across Security, Availability, Processing Integrity, Confidentiality, and Privacy	AICPA
NIST CSF 2.0	Voluntary framework for managing and improving cybersecurity risk posture	NIST / U.S. Dept. of Commerce

Key Takeaways

- SOC 2 Security criteria (CC1–CC9) ≈ NIST CSF Functions (Govern, Identify, Protect, Detect, Respond, Recover).
- Alignment enables “**audit-once, report-many**” compliance.
- AICPA (2024) reported a **36 % YoY increase** in SOC 2 adoptions, underscoring the business value of assurance reporting.
- CSF 2.0 expanded “**Govern (GV)**” Function, formalizing policy and measurement integration.

---

1. Overview of Trust Services Criteria

Category	Description	Common Criteria (CC)
Security	Protection of system resources against unauthorized access (required for all SOC 2 reports)	CC1 – CC9
Availability	Accessibility of systems and data per commitments	CC + A1
Processing Integrity	System processing is complete, valid, accurate, timely, authorized	CC + PI1
Confidentiality	Restricted access and use of confidential information	CC + C1
Privacy	Collection, use, retention, disclosure aligned with entity's privacy notice	CC + P1 – P9

2. NIST CSF 2.0 Core Functions

Function Abbrev.	Function Name	Focus Area Examples
GV	**Govern**	Risk management strategy, policy, roles and responsibilities
ID	**Identify**	Asset management, risk assessment, business environment
PR	**Protect**	Access control, data security, awareness training, maintenance
DE	**Detect**	Monitoring, anomaly detection, continuous security observations
RS	**Respond**	Incident response, mitigation, communications, coordination
RC	**Recover**	Recovery planning, improvement, resilience validation

3. SOC 2 ↔ NIST CSF Cross-Mapping (Practical Reference)

CC1 – Control Environment

Intent: Establish ethical culture and governance structure.
NIST CSF: GV.OC (Org Context), GV.RR (Risk Mgmt Strategy), GV.PO (Policies), GV.OV (Oversight).
Evidence: Code of conduct, policy framework, board minutes, training attestations.

CC2 – Communication & Information

Intent: Enable timely, accurate communication internally and externally.
NIST CSF: GV.CT (Supply-Chain Comms), GV.PO, PR.DS (Data Security), ID.AM (Asset Information).
Evidence: Security awareness materials, vendor notifications, incident templates.

CC3 – Risk Assessment

Intent: Identify objectives, risks, likelihood, and impact.
NIST CSF: GV.RR, ID.RA (Risk Assessment), ID.BE (Business Environment).
Evidence: Risk registers, heat maps, treatment plans, annual review records.

CC4 – Monitoring Activities

Intent: Evaluate control performance and implement corrective actions.
NIST CSF: GV.ME (Measurement & Analysis), DE.MA (Monitoring & Anomalies).
Evidence: Metrics dashboards, audit logs, issue tracking, management reviews.

CC5 – Control Activities

Intent: Translate policy into procedures and approvals.
NIST CSF: PR.AA (Identity & Access Mgmt), PR.AT (Awareness & Training), PR.MA (Maintenance).
Evidence: SOPs, workflow approvals, segregation of duties records.

CC6 – Logical & Physical Access Controls

Intent: Restrict system access to authorized users and devices.
NIST CSF: PR.AA (Access Mgmt), PR.DS (Data Security), PR.PS (Platform Security).
Evidence: MFA configs, access reviews, badge logs, firewall rules, SSO settings.

CC7 – System Operations & Change Management

Intent: Manage changes securely and maintain operational integrity.
NIST CSF: PR.MA, DE.CM (Continuous Monitoring), RS.MI (Mitigation), RC.IM (Improvements).
Evidence: Change tickets, CAB approvals, patch reports, incident logs, rollback tests.

CC8 – Vendor / Third-Party Risk Management

Intent: Assess and monitor outsourced service providers.
NIST CSF: GV.SC (Supply-Chain Risk Mgmt).
Evidence: TPRM policies, vendor risk scores, CAIQ/SIG responses, BAAs.

CC9 – Business Continuity & Resilience

Intent: Ensure continuity of operations and recovery from disruptions.
NIST CSF: RS.PO (Response Planning), RS.CO (Communications), RC.RP (Recovery Plans), RC.CO (Comms).
Evidence: BCP/DR plans, tabletop exercises, RTO/RPO metrics, after-action reports.

---

4. Category-Specific TSC Alignment Highlights

TSC Category	Typical NIST Functions	Example NIST Sub-Categories
Availability (A1)	ID.BE, PR.PS, RC.RP	Backup & redundancy controls, RTO/RPO targets
Processing Integrity (PI1)	PR.MA, DE.CM	Change testing & validation, transaction accuracy

TSC Category	Typical NIST Functions	Example NIST Sub-Categories
Confidentiality (C1)	PR.DS, PR.AA	Encryption key management, access restrictions
Privacy (P1–P9)	ID.BE, PR.DS, GV.RR	Data minimization, purpose limitation, consent records

---

5. AICPA and NIST Market Context (2024–2025)

- **36 % increase** in SOC 2 adoptions across U.S. mid-market companies (AICPA Assurance Survey 2024).
- Over **90 %** of SOC 2 auditors leverage **NIST CSF** for control mapping and testing alignment.
- NIST CSF 2.0 adds "**Govern**" Function and renames ID.AM → PR.AA and PR.PT updates to clarify technology asset scope.
- AICPA emphasizes SOC 2 readiness as a competitive differentiator in RFPs and vendor security assessments.

---

6. Implementation Tips

1. **Establish cross-framework mapping matrix** in your GRC tool (ServiceNow, ZenGRC, or custom Excel).
2. **Tag controls by both criteria** (e.g., CC6.1 ↔ PR.AA-01) to enable dual reporting.
3. **Use NIST Implementation Examples** for SOC 2 testing evidence.
4. **Automate evidence collection** via SIEM, ticketing, and policy repositories.
5. **Perform annual cross-walk reviews** to keep in sync with framework updates.

---

7. References

- AICPA. *(2017, updated 2022).* **Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.** AICPA.org.

- AICPA Assurance & Advisory Innovation Survey 2024 – SOC Reporting Trends.
- NIST. *(2024).* **Cybersecurity Framework 2.0 Core and Implementation Examples.** U.S. Department of Commerce, National Institute of Standards and Technology.
- NIST CSF 2.0 Reference Tool (https://www.nist.gov/cyberframework).

About Iron City IT Advisors

Iron City IT Advisors LLC is a U.S.-based IT and Cybersecurity consulting firm specializing in vCISO and Fractional CISO services, HIPAA and SOC 2 alignment, and NIST CSF maturity roadmaps for healthcare, SaaS, and regulated industries.
Contact: info@ironcityit.com