



Overview: How the CTS Assessment Aligns with SOC 2 Security

Review comparison with AI Controls

The SOC 2 Security Trust Services Criteria (the "Common Criteria," CC1–CC9) is built around nine domains: control environment and governance (CC1), communication and information (CC2), risk assessment (CC3), monitoring of controls (CC4), control activities (CC5), logical and physical access (CC6), system operations (CC7), change management (CC8), and risk mitigation (CC9). The CTS assessment maps cleanly onto every one of these domains and, in most cases, asks for more granular evidence than a SOC 2 Type 2 auditor typically requires for a baseline Security opinion. Across its 176 questions and 20 control buckets, the assessment functions as a superset of CC1–CC9 with additional regulatory, AI, and consumer-interaction depth that SOC 2 Security alone does not require.

Where it meets SOC 2 Security.

The assessment fully covers the foundational logical and physical access criteria (CC6) through its Identification & Authentication bucket (14 questions on MFA, RBAC, least privilege, privileged account inventory, session locks, and joiner-mover-leaver workflows), its Physical & Environmental Security bucket (9 questions on access authorization, visitor escort, CCTV coverage, and 90-day retention), and its Cryptographic Protections bucket (encryption at rest, in transit, for backups, and for non-console admin access). System operations and monitoring (CC7) are addressed by the Continuous Monitoring bucket (SIEM, log retention, time-correlated audit trails, unauthorized-activity detection) and the Incident Response / Vulnerability Management bucket (penetration testing, monthly vulnerability scanning, patch cadence, EOL system tracking). Change management (CC8) is covered by Configuration Management (secure baselines aligned to CIS/MPA/PCI hardening, allowlisting, unauthorized-change detection). Governance and risk (CC1, CC3, CC9) are addressed through the Governance bucket (formal ISMS, annual policy review and management approval), Human Resources Security (background screening, NDAs, rules of behavior, timely access revocation), Third-Party Management (ESP inventory, annual vendor assessments, vendor NDAs), and Business Continuity / DR / IR (contingency plans, RTO/RPO-backed backups, immutable backup verification, integrated IR teams, breach notification timelines). Communication and information (CC2) are handled through Security Awareness Training, including role-based training, social engineering recognition, and consumer-validation training for customer-facing personnel.

Where it exceeds SOC 2 Security.

Several aspects of the assessment go meaningfully beyond what SOC 2 CC1–CC9 demands. First, the Regulatory bucket (14 questions) requires applicability determinations against FTC Act, GLBA 314, SEC Cybersecurity Rule, NYDFS 23 NYCRR 500, Massachusetts 201 CMR 17.00, Illinois BIPA, and 8+ state privacy laws — SOC 2 Security as a framework is regulation-agnostic and does not require this jurisdictional analysis. Second, the AI bucket (16 questions) covers AI governance, risk tolerance, oversight committees, regulatory mapping for AI tools, model accuracy/bias monitoring intervals, and consumer-data-in-AI restrictions; this aligns more closely with NIST AI RMF and ISO 42001 than with SOC 2, which has no native AI criteria. Third, Consumer Information Risk (5 questions on NPI handling, monitored vs. unmonitored consumer interaction) and elements of Data Classification (clean desk policies, mobile device bans on operations floors, call recording) reflect a contact-center / consumer-facing operational posture that SOC 2 typically would only address if the customer scoped Confidentiality or Privacy criteria in addition to Security. Fourth, the CISA Top 10 bucket and the requirement to upload an actual penetration test report, BCP/DR test evidence, and backup restoration validation dates push the assessment toward operational verification rather than control-design attestation, which exceeds the design-and-operating-effectiveness bar of CC4.

The bottom line.

A vendor that can answer this CTS assessment satisfactorily would, in nearly all cases, also satisfy SOC 2 Security CC1–CC9 — the inverse is not necessarily true. The assessment is best characterized as SOC 2 Security plus regulatory applicability, plus AI governance, plus consumer-interaction operational controls. The two notable areas where SOC 2 Type 2 would still add value beyond this questionnaire are (1) independent third-party attestation by a licensed CPA firm with documented testing procedures and sample sizes, and (2) the formal opinion on operating effectiveness over a defined period (typically 6–12 months), which a self-attested questionnaire cannot replicate. For a vendor risk decision, the CTS assessment is stronger evidence base than a SOC 2 Security report alone for technical and regulatory coverage, but it pairs best with a SOC 2 Type 2 to validate that the controls described are actually operating as stated over time.