COMPLIANCE ALIGNMENT GUIDE

Total Access Control (TAC) and SOC 2

How TAC's architecture and capabilities map to the AICPA Trust Service Criteria

PortSys, Inc. | www.portsys.com

Overview

SOC 2 (Service Organization Control 2) is a compliance framework developed by the American Institute of Certified Public Accountants (AICPA) that evaluates how organizations manage data based on five Trust Service Criteria: **Security**, **Availability**, **Processing Integrity**, **Confidentiality**, and **Privacy**.

Security is the only mandatory criterion — the remaining four are selected based on the services an organization provides. SOC 2 Type II audits evaluate whether controls operated effectively over a sustained period, not just at a single point in time.

Total Access Control (TAC) by PortSys directly addresses the most critical SOC 2 control requirements through its unified zero-trust access platform. This document maps TAC’s architecture and capabilities to each of the five Trust Service Criteria.

---

1. Security (Common Criteria) — Required

Security is the foundation of every SOC 2 audit. TAC addresses the most critical control categories directly.

Logical Access Controls (CC6)

SOC 2 Requirement	How TAC Delivers
Restrict logical access to authorized users	**Reverse-proxy enforcement** — no user connects directly to any application. TAC mediates every access request before traffic reaches the target resource.
Authenticate users before granting access	**Built-in MFA** including FIDO2, SafeLogin MFA, TOTP, push notifications, SMS, OTP, and hardware tokens — plus integration with virtually any third-party MFA provider including Duo, RSA, Swivel, biometric solutions, and others.
Require multi-factor authentication	**7+ MFA methods** included in the base TAC license. No add-on purchases required to satisfy auditor MFA requirements.
Manage credentials and access rights	**Multi-directory identity federation** connects simultaneously to Active Directory, LDAP, SAML, RADIUS, OIDC, SQL databases, and custom directories — all governed by a single unified policy engine.
Revoke access when no longer authorized	**Real-time access revocation** when device compliance lapses, policy conditions change, or identity status is modified — mid-session, not just at next login.
Implement role-based access control	**Unified policy engine** enforces access decisions based on user identity, group membership, device posture, application, network location, time of day, and risk signals.

System Operations and Monitoring (CC7)

SOC 2 Requirement	How TAC Delivers
Monitor system components for anomalies	**Complete audit trail** of every access request — who accessed what, when, from where, from which device, and what policy allowed or denied it.
Detect unauthorized access attempts	Every request is evaluated against policy in real time. **Unauthorized**

SOC 2 Requirement	How TAC Delivers
	attempts are logged and blocked at the proxy layer before reaching the target application.
Maintain audit logs	**Forensic-grade logging** for every human user and AI agent action, with full identity attribution and policy decision recording.

Risk Mitigation (CC5)

SOC 2 Requirement	How TAC Delivers
Identify and mitigate risks to system security	**Attack surface reduction** — close every inbound firewall port except one single encrypted channel supporting up to TLS 1.3.
Protect against external threats	**Stealth infrastructure** — applications are never directly exposed to the internet. Attackers cannot discover, scan, or directly reach protected resources.
Manage vulnerabilities in endpoints	**Continuous device posture validation** checks OS patches, antivirus status, disk encryption, firewall status, domain join, and certificate validity on every request — not just at login.

---

2. Availability

SOC 2 Requirement	How TAC Delivers
Ensure system availability and redundancy	**SVA Array architecture** provides multiple load-balanced appliances for high availability. Global Array extends redundancy across worldwide data center locations.
Support disaster recovery objectives	**Single-tenant deployment** means

SOC 2 Requirement	How TAC Delivers
	your disaster recovery strategy is under your control — not dependent on a shared vendor cloud or subject to another organization's failover events.
Minimize unplanned downtime	**Deploy in hours, not months.** Failover configurations, load balancing, and health monitoring are managed from a single admin console.
Maintain business continuity	**Location-transparent SSO** ensures applications can migrate between on-premises and cloud environments without user disruption or access interruption.

---

3. Confidentiality

SOC 2 Requirement	How TAC Delivers
Protect confidential information from unauthorized access	**Single-tenant Secure Virtual Appliance (SVA) architecture** ensures complete data isolation. No shared infrastructure. No data co-mingling with other organizations — ever.
Limit access to authorized personnel only	**Unified policy engine** restricts access by identity, device posture, network location, time of day, and application — down to individual resources and API endpoints.
Encrypt data in transit	All traffic flows through a **single port encrypted up to TLS 1.3**. No unencrypted channels. No exposed application ports.
Classify and control access to sensitive data	**Differentiated access rules** per application, resource, user group, and identity type — including separate policies for AI agents and automated workflows.
Protect legacy systems containing	**Reverse-proxy authentication**

SOC 2 Requirement	How TAC Delivers
confidential data	**injection** adds MFA, device posture checks, and continuous validation to legacy applications — without modifying the application or its code.

---

4. Processing Integrity

SOC 2 Requirement	How TAC Delivers
Ensure system performs intended functions without error	**Per-request policy evaluation** ensures every access decision is consistent, auditable, and repeatable — driven by the same policy engine for every request.
Prevent unauthorized modification of data	**Reverse-proxy architecture** ensures applications never process requests that have not passed identity verification, device posture validation, and policy evaluation.
Ensure complete and accurate processing	**Complete audit trail** with timestamps, identity attribution, device details, and policy decision logging for every access transaction.

---

5. Privacy

SOC 2 Requirement	How TAC Delivers
Protect personal information	**Single-tenant isolation** ensures personal data processed by your applications never co-mingles with other customers' environments.
Control access to systems containing personal data	**Granular policy enforcement** controls which users and AI agents can access systems containing PII, PHI, or

SOC 2 Requirement	How TAC Delivers
	other regulated data.
Monitor and log access to sensitive systems	**Complete logging** of every access event — who accessed which application, when, from what device, and the policy decision that allowed or denied access.

Why TAC Is Uniquely Strong for SOC 2

Three architectural advantages set TAC apart from competing solutions in a SOC 2 audit context:

Single-Tenant Isolation

Auditors consistently flag multi-tenant architecture as a risk factor — shared infrastructure creates potential for cross-customer data exposure, noisy-neighbor performance impacts, and shared-fate security incidents. TAC eliminates these concerns entirely. Every TAC deployment is a dedicated, isolated Secure Virtual Appliance. There is no shared infrastructure. Auditors can verify this directly.

One Console, One Audit Trail

Most organizations assemble SOC 2 evidence from 3–6 separate tools — identity provider logs, MFA provider logs, VPN logs, endpoint management logs, and application access logs. This fragmentation is itself a control gap that auditors flag. TAC provides a single, unified audit trail covering identity, MFA, device posture, and access decisions. Evidence collection during audit becomes dramatically simpler.

Continuous Validation, Not Point-in-Time

SOC 2 Type II audits evaluate whether controls operated effectively over time — not just at a single moment. TAC's per-request device posture validation and continuous policy evaluation mean compliance is enforced on every access request throughout the audit period. If a device falls out of compliance mid-session, access is revoked immediately. This is exactly the operating effectiveness that Type II auditors want to see documented.

Control Coverage Summary

Trust Service Criterion	Required?	TAC Coverage
Security (Common Criteria)	Yes — Required	**Comprehensive.** Reverse-proxy enforcement, built-in MFA, continuous device posture, unified policy engine, full audit logging, attack surface reduction.
Availability	Optional	**Strong.** SVA Array and Global Array for HA and redundancy. Single-tenant deployment for customer-controlled DR. Hours-not-months deployment.
Processing Integrity	Optional	**Addressed.** Per-request policy evaluation ensures consistent, auditable, repeatable access decisions with complete transaction logging.
Confidentiality	Optional	**Comprehensive.** Single-tenant isolation, TLS 1.3 encryption, granular access policies, legacy app security uplift, AI agent governance.
Privacy	Optional	**Addressed.** Dedicated infrastructure isolation, granular access control for systems containing personal data, complete access logging.

Next Steps

To learn more about how TAC aligns with your specific SOC 2 audit requirements:

- Request a personalized compliance walkthrough at www.portsys.com/contact
- Download the TAC Product Datasheet for full capability details
- Ask about TAC deployment in your specific compliance environment

---

This document is provided for informational purposes and describes how TAC’s capabilities map to SOC 2 Trust Service Criteria. SOC 2 compliance is determined by independent auditors based on your organization’s complete control environment, of which TAC is one component.