COMPLIANCE ALIGNMENT GUIDE

Total Access Control (TAC) and PCI-DSS v4.0

How TAC's architecture and capabilities map to PCI-DSS v4.0 requirements for controlling access to the applications and systems within your cardholder data environment.

Audience	Standard	Version
CISOs, compliance leads, QSAs, security architects	PCI-DSS v4.0 — Requirements 1, 7, 8, 10, 11	v2.0 — 2026

Overview

The Payment Card Industry Data Security Standard (PCI-DSS) v4.0 establishes comprehensive requirements for organisations that process, store, or transmit cardholder data. With enforcement of v4.0 fully in effect, organisations must demonstrate robust controls across network security, access management, authentication, monitoring, and security testing.

Total Access Control (TAC) by PortSys directly addresses several PCI-DSS v4.0 requirements — particularly in network security controls (Req 1), access restriction (Req 7), multi-factor authentication (Req 8), and logging and monitoring (Req 10) — for the applications and systems within your cardholder data environment (CDE). TAC's reverse-proxy architecture also reduces the external attack surface relevant to security testing (Req 11).

TAC Scope in PCI-DSS. TAC controls **access to applications and systems within the CDE** — administrative consoles, operations tools, customer service portals, dashboards, and other applications that interact with cardholder data. TAC addresses Requirements 1, 7, 8, 10 for systems in scope, and reduces the attack surface that Requirement 11 scans must cover.

TAC does **not** encrypt PAN at rest, tokenise cardholder data, mediate payment processing, replace network segmentation, or perform vulnerability scans or penetration testing. Requirements such as Req 3 (storage), Req 4 (CHD transmission), Req 5 (anti-malware), Req 6 (secure development), and Req 12 (organisational policies) are satisfied by other controls in your environment.

PCI-DSS v4.0 Control Mapping

Each requirement below is matched to a specific TAC capability for the applications TAC fronts.

NETWORK PROTECTION

Requirement 1 — Network Security Controls

REQUIREMENT	HOW TAC DELIVERS
1.2.1 — Configuration standards for network security controls	TAC's Secure Virtual Appliance (SVA) provides a hardened, single-purpose reverse-proxy platform. Configuration is centralised through a single admin console, ensuring consistent security control standards across all TAC-fronted CDE applications.
1.2.5 — All services, protocols, and ports allowed are identified and approved	TAC reduces this requirement for fronted applications to its simplest form: close all inbound firewall ports except one encrypted port (TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules). Every protected application — web, thick-client, forms-based, API — is accessed through this single port. No other inbound services, protocols, or ports for these applications need approval because none are open.
1.3.1 — Inbound traffic to the CDE is restricted	Inbound traffic to TAC-fronted CDE applications passes through a single encrypted channel. Applications behind TAC are not directly addressable from any network. All traffic is authenticated, authorised, and policy-validated before reaching the application. (Note: TAC complements but does not replace network segmentation between CDE and non-CDE networks.)
1.4.1 — Network security controls between trusted and untrusted networks	TAC functions as a network security control between untrusted networks (internet, remote users) and the trusted CDE applications it fronts. The reverse proxy evaluates every connection request against identity, MFA, device posture, and policy before permitting access.

ACCESS CONTROL

Requirement 7 — Restrict Access by Business Need

REQUIREMENT	HOW TAC DELIVERS
7.2.1 — Access control model defined for each system component	TAC's unified policy engine provides a centralised access control model covering every CDE application accessible through the platform. Policies are defined based on role, group membership, device compliance, geolocation, time of day, and application sensitivity.
7.2.2 — Access assigned based on job classification and function	Multi-directory identity federation (Active Directory, LDAP, SAML, RADIUS, OIDC, SQL, custom directories) enables role-based and attribute-based access assignment drawn directly from organisational directories and HR systems.
7.2.4 — Application and system accounts (service accounts, AI agents)	Non-human identities — service accounts, API clients, and AI agents accessing CDE applications — governed by the same identity, policy, and audit framework as human users. No separate identity silo for programmatic access. Critical for environments where AI agents and integrations interact with cardholder data systems.

REQUIREMENT	HOW TAC DELIVERS
7.2.5 — All access privileges assigned and managed	Single admin console manages all access policies. Changes to access privileges are immediately enforced across all TAC-fronted applications. Revoking directory access immediately terminates TAC access.

AUTHENTICATION

Requirement 8 — Identify Users and Authenticate Access

REQUIREMENT	HOW TAC DELIVERS
8.2.1 — All users assigned a unique ID	Multi-directory identity federation ensures unique user identification across all directory sources. Both human and non-human (service account, AI agent) identities receive unique identification.
8.2.2 — Shared / group accounts not used	TAC's identity federation enforces individual authentication. Each user authenticates with their own unique credentials and MFA, even when accessing shared applications.
8.3.1 — All user access authenticated with at least one authentication factor	Every access request through TAC requires authentication. No unauthenticated access paths exist — the reverse-proxy architecture ensures all traffic passes through identity verification.
8.4.1 — MFA for all non-console administrative access into the CDE	TAC enforces MFA for all access to TAC-fronted CDE applications — administrative and user alike. Built-in MFA includes FIDO2 / WebAuthn (phishing-resistant), SafeLogin (proprietary), TOTP, push notifications, SMS, OTP, and hardware tokens. Third-party MFA integration with virtually any provider including Duo, RSA, Swivel, biometric solutions, and others.
8.4.2 — MFA for all access into the CDE	MFA enforced by default for all access through TAC, not just administrative access. Applies per-request, not just at login. All MFA methods included in the base licence — no per-user surcharges or add-on tiers.
8.4.3 — MFA for all remote network access originating from outside the entity's network	TAC is purpose-built for secure remote access to CDE applications. All remote connections pass through MFA, device posture validation, and policy evaluation. Phishing-resistant FIDO2 / WebAuthn is available for the strongest remote authentication.
8.6.1 — System and application accounts managed and secured	Service-account credentials and AI-agent identities are first-class citizens in the same policy engine that governs human access. Programmatic identities are authenticated and policy-evaluated on every request, just like human users. No separate authentication path for non-human access to protected CDE applications.
Continuous device posture as authentication context	Device posture validation extends authentication beyond just ‘who you are’ to ‘what device you are using’ — checking OS version, patch level, antivirus status, disk encryption, firewall status, and domain join status. Non-compliant devices are denied access in real time on every request, not just at login. If device compliance lapses mid-session, access is revoked immediately.

AUDIT LOGGING

Requirement 10 — Log and Monitor All Access

REQUIREMENT	HOW TAC DELIVERS
10.2.1 — Audit logs enabled and active for all system components in the CDE	TAC generates comprehensive audit logs for every access request to TAC-fronted CDE applications. Logging is automatic and cannot be disabled — no configuration required to capture baseline events.
10.2.1.1 — Audit logs capture all individual user access to cardholder data applications	Every access request is logged with: user identity, authentication method, device posture status, source IP, geolocation, timestamp, application accessed, policy decision (allow / deny / step-up), and session duration. Both human users and non-human (service account, AI agent) access are logged.
10.2.1.2 — Audit logs capture all actions taken by any individual with administrative access	Administrative actions within the TAC console are logged separately. Combined with access logs, this provides complete audit trail coverage for the platform.
10.2.1.5 — Audit logs capture all changes to identification and authentication credentials	MFA enrolment, modification, and revocation events are logged. Identity federation configuration changes are captured in the audit trail.
10.2.2 — Audit logs record required details for each auditable event	Each log entry includes: user identification, type of event, date and time, success or failure indication, origination of event (IP, geolocation, device), and identity or name of affected application / resource.
10.4.1 / 10.7 — Audit logs reviewed and suspicious activity responded to	Failed authentications, policy violations, and device compliance failures are logged in real time. TAC provides native real-time monitoring and alerting on these events for the applications it protects. Logs also export to your SIEM via syslog or API for downstream correlation, retention, and forensic analysis.
10.5.1 — Retain audit logs for at least 12 months	TAC audit logs support configurable retention policies meeting PCI-DSS 12-month minimum requirements, with at least three months immediately available for analysis.

SECURITY TESTING

Requirement 11 — Test Security of Systems and Networks

Scope note. TAC does not perform vulnerability scans or penetration testing. Requirement 11.3 (quarterly internal and external scans) and 11.4 (penetration testing) still apply to all systems in scope. TAC's contribution is reducing the external attack surface that those scans must cover.

REQUIREMENT	HOW TAC DELIVERS
11.3.1 / 11.3.2 — Internal and external vulnerability scans	TAC does not replace the quarterly scan requirement. By closing all inbound ports except one encrypted channel for TAC-fronted applications, the **external attack surface presented to scans is reduced to the TAC entry point itself**. Internal scans of CDE systems behind TAC still apply per PCI-DSS scope rules.
11.5 — Change-detection mechanisms	TAC's audit logs detect changes to access policies, identity-source bindings, and authentication configuration. (Note: this is change detection on the access control layer, not file integrity monitoring on CDE system files.)

Why TAC Is Uniquely Strong for PCI-DSS

Close All Ports — Shrink the Access Attack Surface

PCI-DSS Requirement 1 demands robust network security controls. TAC closes all inbound firewall ports except one encrypted channel (TLS 1.2 or TLS 1.3 with FIPS 140-2 modules) for the CDE applications it fronts. Administrative consoles, operations tools, and customer service portals handling cardholder data are not directly exposed to the internet. Most competing approaches leave datacenter ports open behind their cloud or concentrator — TAC closes them.

Legacy Application Protection

Many payment processing organisations operate critical CDE applications on legacy systems that cannot natively support MFA or modern authentication. TAC injects MFA, device posture, and continuous validation in front of any application — without changing a single line of code or requiring re-certification.

Single-Tenant Isolation

Every TAC deployment is a dedicated, isolated Secure Virtual Appliance — on-premises, in your cloud account, or hybrid. Access policies and audit data for your CDE never co-mingle with another organisation's environment. This matters where shared-cloud architecture creates QSA or board-level concerns.

All-Inclusive Licensing — No Compliance Gaps

TAC includes every security feature in the base licence: all MFA methods, device posture validation, AI agent governance, SSO, and 24×7 support. No add-on tiers, no per-user MFA surcharges, no premium feature gates. Eliminates the common PCI risk where organisations skip critical security controls because they are priced as premium add-ons.

Reduce CDE Scope Through Architecture

TAC's reverse-proxy architecture can help reduce PCI-DSS scope by consolidating all access to CDE applications through a single, well-controlled access point. By mediating every connection, TAC creates a clear boundary between the CDE applications in scope and the rest of the network — simplifying scope definition and documentation for QSAs.

PCI-DSS v4.0 Coverage Summary

CONTROL FAMILY / FRAMEWORK	CONTROLS ADDRESSED	TAC COVERAGE
Requirement 1	Network Security Controls	Reverse-proxy with single encrypted port, stealth infrastructure for fronted applications, NSCs between trusted/untrusted networks
Requirement 7	Restrict Access by Business Need	Unified policy engine, role-based and attribute-based access, service accounts & AI agents, immediate revocation
Requirement 8	Identify and Authenticate	Multi-directory federation, built-in & third-party MFA, device posture, continuous validation, service accounts
Requirement 10	Log and Monitor	Comprehensive attributed audit trail, native real-time monitoring & alerting, optional SIEM export
Requirement 11	Security Testing (partial)	Reduces external attack surface scans must cover; does not replace quarterly scan or penetration testing requirements

Next Steps

Map your CDE application inventory. Identify every administrative console, operations tool, portal, dashboard, and integration that accesses cardholder data. Each is a candidate for TAC mediation.

Request a PCI-DSS compliance walkthrough. A PortSys specialist will walk through your specific environment, identify high-priority CDE applications, and produce a prioritised deployment plan with timeline and milestones.

Contact: portsys.com/contact | info@portsys.com

This document maps TAC capabilities to PCI-DSS v4.0 requirements. PCI-DSS compliance is validated by a Qualified Security Assessor (QSA) or via Self-Assessment Questionnaire (SAQ) against the complete organisational security programme. TAC is one component of that programme — PortSys recommends working with a QSA and qualified PCI advisors.