COMPLIANCE ALIGNMENT GUIDE

Total Access Control (TAC) and ISO 27001

How TAC's architecture and capabilities support ISO/IEC 27001:2022 Annex A controls — particularly access control, authentication, network security, cryptography, and monitoring.

Audience	Framework	Version
ISMS managers, CISOs, ISO 27001 certification candidates, surveillance audit teams	ISO/IEC 27001:2022 Annex A	v2.0 — 2026

TAC Scope in ISO 27001. TAC supports specific Annex A technical controls — access control (A.5.15-A.5.18), supplier access (A.5.19, A.5.22), authentication and secure access (A.8.2, A.8.3, A.8.5), logging and monitoring (A.8.15, A.8.16), network security (A.8.20, A.8.21, A.8.22), and cryptography (A.8.24). TAC produces the technical evidence ISO 27001 lead auditors expect for these controls.

TAC does **not** replace the Information Security Management System (ISMS), nor address physical security (A.7), most people controls (A.6), organisational policies, software development controls (A.8.25-A.8.28), information classification or labelling (A.5.12, A.5.13), or content-level data leakage prevention (A.8.12). ISO 27001 certification is granted by accredited certification bodies based on the complete ISMS, of which TAC is one technical component.

Overview

ISO/IEC 27001:2022 is the international standard for Information Security Management Systems (ISMS). It provides a systematic approach to managing sensitive company information across people, processes, and technology. Certification requires demonstrating that controls from Annex A have been implemented and operate effectively over time across four themes: Organisational (A.5), People (A.6), Physical (A.7), and Technological (A.8).

Total Access Control (TAC) by PortSys addresses specific Annex A controls within the Organisational and Technological themes — particularly access control, authentication, network security, cryptography, and monitoring — for the applications and systems it fronts.

ACCESS CONTROL

A.5.15 — A.5.18

REQUIREMENT	HOW TAC DELIVERS
A.5.15 — Access control policy	TAC's unified policy engine centralises all access decisions into a single console. Policies are defined by identity, device posture, application, network location, time of day, and risk signals — ensuring consistent enforcement across all protected resources.

REQUIREMENT	HOW TAC DELIVERS
A.5.16 — Identity management	Multi-directory identity federation connects simultaneously to Active Directory, LDAP, SAML, RADIUS, OIDC, SQL databases, and custom directories. Human users, service accounts, and AI agent identities are managed through one policy framework.
A.5.17 — Authentication information	Built-in MFA includes FIDO2 / WebAuthn (phishing-resistant), SafeLogin (proprietary), TOTP, push notifications, SMS, OTP, and hardware tokens. Integrates with virtually any third-party MFA provider including Duo, RSA, Swivel, biometric solutions, and others. All methods included in base licence.
A.5.18 — Access rights	Granular role-based and attribute-based access control. Access rights enforced per request at the reverse-proxy layer. Real-time revocation when policy conditions change or device compliance lapses — mid-session, not just at next login.

SUPPLIER AND THIRD-PARTY ACCESS

A.5.19 — A.5.22

REQUIREMENT	HOW TAC DELIVERS
A.5.19 — Information security in supplier relationships	Single-tenant Secure Virtual Appliance (SVA) architecture ensures your TAC deployment is completely isolated from all other customers. No shared infrastructure, no data co-mingling. Third-party AI agents and supplier accounts governed by the same policy engine as internal users.
A.5.22 — Monitoring of supplier services	Customer-controlled deployment (on-premises, private cloud, public cloud, or hybrid) gives you direct control over monitoring, logging, and auditing of the TAC platform itself. Vendor remote access sessions can be time-bounded, scoped, and individually logged.

AUTHENTICATION AND SECURE ACCESS

A.8.2 — A.8.5

REQUIREMENT	HOW TAC DELIVERS
A.8.2 — Privileged access rights	TAC enforces differentiated policies for privileged users, including stronger MFA requirements, stricter device posture checks, and time-bounded access windows. AI agent access to privileged systems is governed with resource-level permissions and full audit.
A.8.3 — Information access restriction	Reverse-proxy architecture ensures applications are never directly accessible. Every request passes through identity verification, MFA challenge, device posture validation, and policy evaluation before reaching the target resource.

REQUIREMENT	HOW TAC DELIVERS
A.8.5 — Secure authentication	Phishing-resistant FIDO2 / WebAuthn authentication included. Continuous authentication through per-request device posture validation — not just at initial login. MFA applies to legacy applications that cannot natively support modern authentication.

LOGGING AND MONITORING

A.8.15 — A.8.16

REQUIREMENT	HOW TAC DELIVERS
A.8.15 — Logging	Comprehensive audit trail of every access request: identity (human, service account, or AI agent), device posture, source IP, geolocation, timestamp, application accessed, and policy decision (allow / deny / step-up). Logging is automatic and cannot be disabled for protected applications.
A.8.16 — Monitoring activities	Native real-time monitoring and alerting on access events and platform health. Continuous policy evaluation on every request enables continuous monitoring; non-compliant devices or policy violations trigger immediate session revocation. Centralised audit data exportable via syslog or API to your SIEM.

NETWORK SECURITY

A.8.20 — A.8.22

REQUIREMENT	HOW TAC DELIVERS
A.8.20 — Networks security	TAC's reverse-proxy architecture routes all application traffic through a single encrypted channel using TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules. All other inbound firewall ports are closed, dramatically reducing the network attack surface.
A.8.21 — Security of network services	Single-tenant Secure Virtual Appliance architecture provides dedicated, isolated infrastructure. No shared multi-tenant services. Scales from single SVA to SVA Array to Global Array for high availability and geographic distribution.
A.8.22 — Segregation of networks	Reverse-proxy enforcement creates logical segregation between user networks and protected application zones. Applications are never directly exposed to user-facing networks; every connection is mediated by TAC's policy engine. Network-level reachability is decoupled from authorisation — being on a network doesn't grant access to anything.

CRYPTOGRAPHY

A.8.24

REQUIREMENT	HOW TAC DELIVERS
A.8.24 — Use of cryptography	All traffic to and from protected applications encrypted via TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules. Single encrypted channel for all application access; no unencrypted protocols permitted. Certificate management and validation are included in device posture checks. (Note: TAC addresses cryptographic protection in transit; cryptographic protection at rest requires complementary application or storage-layer controls.)

Why TAC Is Strong for ISO 27001

Unified Technical Control Implementation. ISO 27001 requires demonstrating that controls are implemented and operate effectively — not just documented. TAC consolidates access control, authentication, device posture, network security, and access monitoring into one platform, making it straightforward to demonstrate implementation to lead auditors across multiple Annex A requirements simultaneously.

Continuous Effectiveness Evidence. Certification audits and surveillance audits evaluate whether controls operate effectively over time. TAC's per-request policy evaluation and continuous device posture validation generate ongoing evidence of control effectiveness — not periodic snapshots that leave gaps between assessments. Mid-session revocation when device compliance lapses produces evidence of real-time enforcement.

Reduced Audit Scope Complexity. Organisations using 3-6 separate tools for authentication, MFA, device posture, network access, and logging face exponentially more complex audit scoping. TAC replaces multiple tools with a single platform, reducing the number of systems lead auditors need to evaluate and the volume of evidence that needs to be collected.

Single-Tenant Isolation for Confidentiality Evidence. ISO 27001's confidentiality expectations are easier to evidence when the access control infrastructure is single-tenant. Every TAC deployment is a dedicated, isolated SVA — auditors can verify this directly rather than rely on vendor attestations about multi-tenant separation.

Legacy Application Authentication Uplift. Many organisations pursuing ISO 27001 certification operate legacy applications that cannot natively support modern authentication. TAC injects MFA, device posture, and continuous validation in front of any application — without changing a single line of code — bringing legacy systems up to current control expectations.

Annex A Coverage Summary

CONTROL FAMILY / FRAMEWORK	CONTROLS ADDRESSED	TAC COVERAGE
Access Control	A.5.15 — A.5.18	Policy, identity management, authentication information, access rights
Supplier Access	A.5.19, A.5.22	Single-tenant isolation, customer-controlled deployment, vendor access governance
Authentication & Secure Access	A.8.2 — A.8.5	Privileged access, information access restriction, secure authentication (FIDO2)
Logging & Monitoring	A.8.15 — A.8.16	Comprehensive audit trail, native real-time monitoring, SIEM export
Network Security	A.8.20 — A.8.22	Single-port architecture, single-tenant SVA, reverse-proxy network segregation
Cryptography	A.8.24	TLS 1.2/1.3 with FIPS 140-2 compliant cryptographic modules (in transit)

Next Steps

Identify Annex A controls in your Statement of Applicability. Map the controls your ISMS scope requires to the technical evidence TAC produces. **Request an ISO 27001 walkthrough** at portsys.com/contact or info@portsys.com — a PortSys specialist will work through your specific environment and produce a prioritised deployment plan with the technical-evidence package your lead auditor will expect.