SOC 2 Readiness Report

Management self-assessment mapped to the AICPA Trust Services Criteria.
Not a SOC 2 Type I or Type II report.

Privion
Assessment as of May 22, 2026
Framework: AICPA Trust Services Criteria (2017)
Trust Center: https://priviontech.com/trust

Document generated May 22, 2026

Overview

This document is a management readiness self-assessment mapped to the AICPA Trust Services Criteria. It is not a SOC 2 Type I or Type II report and has not been examined or attested to by an independent certified public accountant. Privion does not represent that controls are suitably designed or operating effectively for audit purposes until a completed engagement with a qualified service auditor.

Trust Service Categories in scope

- Security (Common Criteria CC1–CC9)
- Availability (A1)
- Confidentiality (C1)

Audit roadmap

- SOC 2 Type 1 — target Q4 2026.
- SOC 2 Type 2 — target Q3 2027.

Assessment summary

Of 11 criteria summaries in this report: 5 implemented, 6 partially implemented, 0 planned.

System description

Privion helps organizations modernize Microsoft 365 environments and operates hosted services. Privion's SOC 2 scope is intended to cover (1) the Privion Intranet hosted service, (2) the PAnalytics hosted service, and (3) the privileged-access program by which Privion personnel access client Microsoft 365 tenants. It does not cover client tenants themselves, which remain the client's responsibility.

Services in scope

- Microsoft 365, SharePoint, and Power Platform consulting performed in client tenants (privileged-access program only; client data remains in the client tenant).
- Privion Intranet — structured outputs via cloud AI on Privion-managed Azure (West US 2); proprietary methodology; encrypted transit; no persistent client content after delivery; no training re-use.
- PAnalytics — Privion-hosted Matomo on shared Azure West US 2; nightly MySQL dumps replicated to Azure Blob Storage in Azure West Central US (30-day retention) with documented restore procedure.
- Privion corporate systems supporting the above (identity, collaboration, billing, and security operations).

Trust boundaries

- Consulting: Privion does not store or relocate client Microsoft 365 content; risk surface is partner-delegated administrative access (GDAP) and project-scoped access.
- Hosted services (Privion Intranet and PAnalytics): Privion acts as data processor for data processed in those environments.

- Subprocessors and platform inheritance: Microsoft Azure and Microsoft 365 provide underlying infrastructure controls (SOC 2 Type II / ISO 27001 at platform level). Additional subprocessors are listed at priviontech.com/trust/subprocessors.

Principal service commitments

- MFA for all personnel; FIDO2 for tenant-admin operations; Entra PIM for just-in-time elevation; GDAP for client tenant access without standing Global Administrator.
- Encryption in transit (TLS 1.2+) and at rest per Azure defaults for hosted storage; PAnalytics nightly cross-region MySQL dump backups (30-day retention).
- Managed company devices for administrative work: full-disk encryption, MFA, and SSH-key infrastructure access; Intune and Defender for Endpoint phased through 2026.
- Annual security awareness training; FCRA-aligned background screening for personnel with client access.
- Incident response and customer notification procedures published at priviontech.com/trust/incident-response.

Criteria mapping

The table below summarizes how Privion control activities align to selected Trust Services Criteria points of focus. Status reflects management judgment as of the assessment date.

CC1 — Control environment (Implemented)

Security — Common Criteria. The entity demonstrates a commitment to integrity and ethical values and establishes structures, reporting lines, and responsibilities for security.

- Documented information security program and policy set (public summaries at priviontech.com/trust/policies).
- Security ownership and escalation via security@priviontech.com and published IR contact paths.
- Background screening for personnel with client tenant access.

CC2 — Communication and information (Implemented)

Security — Common Criteria. The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

- Trust Center and compliance pages communicate scope, subprocessors, and control summaries to customers.
- Annual security awareness training for all personnel; completion evidence available upon request.
- Policy communication and subsidiary policy linkage in the information security policy summary.

CC3 — Risk assessment (Partially implemented)

Security — Common Criteria. The entity specifies objectives with sufficient clarity and identifies risks to the achievement of those objectives.

- Trust-boundary framing separates client-tenant consulting from hosted processor environments.
- SOC 2 readiness program tracks gaps and remediation ahead of planned Type 1 / Type 2 audits.
- Vendor/subprocessor inventory with DPA expectations in vendor management policy summary.

Notes: Formal enterprise risk register maturation continues through the audit readiness program.

CC4 — Monitoring activities (Partially implemented)

Security — Common Criteria. The entity selects, develops, and performs ongoing and/or separate evaluations and remedies deficiencies.

- Azure Monitor for hosted infrastructure; quarterly client tenant access reviews.
- Patch cadence: critical updates within 14 days on managed endpoints.

Notes: Organization-wide SIEM and advanced detection capabilities are not deployed; monitoring relies on platform tooling today.

CC5 — Control activities (Implemented)

Security — Common Criteria. The entity selects and develops control activities that contribute to the mitigation of risks.

- Access control, data classification, acceptable use, vendor management, and business continuity policy summaries.
- Conditional Access on administrative accounts; secure disposal at engagement end.

CC6 — Logical and physical access (Implemented)

Security — Common Criteria. The entity implements logical access security software, infrastructure, and architectures over protected information assets.

- MFA for all personnel; FIDO2 for tenant-admin roles; Entra PIM; GDAP (no standing Global Administrator).
- Quarterly access reviews per client tenant; GDAP/PIM recovery playbooks with annual review.
- Client admin work restricted to managed devices via Conditional Access.

CC7 — System operations (Partially implemented)

Security — Common Criteria. The entity manages the operation of system(s) and implements detection and monitoring processes.

- Hosted services in Azure West US 2; PAnalytics (Privion-hosted Matomo) with cross-region backup to Azure West Central US.
- Managed endpoints with encryption, MFA, and SSH-key access for infrastructure administration; patch and host-security baselines enforced.
- Incident response policy summary and public IR overview.

Notes: Microsoft Intune and Defender for Endpoint phased deployment through 2026 for centralized management and monitoring.

CC8 — Change management (Partially implemented)

Security — Common Criteria. The entity authorizes, designs, develops, configures, documents, tests, approves, and implements changes.

- Infrastructure and application changes for hosted services follow documented change practices tied to Azure deployment pipelines.
- Policy and Trust Center updates versioned with last-updated dates.

Notes: Formal change-advisory documentation continues to mature for the audit program.

CC9 — Risk mitigation (Partially implemented)

Security — Common Criteria. The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

- Business continuity and disaster recovery policy summary for hosted services.
- PAnalytics: nightly mysqldump to Azure Blob Storage in Azure West Central US (30-day retention); documented restore procedure; quarterly recovery test; RTO/RPO available on request.
- Platform-level resilience inherited from Microsoft Azure.

Notes: PAnalytics RTO/RPO provided on request; org-wide penetration test planned 2027.

A1 — Availability commitments and system availability (Partially implemented)

Availability. The entity maintains, monitors, and evaluates current processing capacity and availability commitments.

- Azure hosting for hosted services with documented region (West US 2).
- Backup and restoration planning described in business continuity policy summary and Trust Center.
- Historical hosted-service availability strong; no contractual uptime SLA published on the Trust Center.

Notes: PAnalytics RTO/RPO available on request; quarterly recovery test per documented procedure. No contractual uptime SLA on Trust Center today.

C1 — Confidential information protection (Implemented)

Confidentiality. The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

- Data classification policy summary; TLS 1.2+ in transit; encryption at rest for hosted storage.
- Privion Intranet: proprietary methodology; documents and intermediate artifacts not retained after delivery; no training re-use.
- DPA and subprocessors available on request; GDPR/CCPA-aligned configurations for PAnalytics where applicable.

Planned milestones

- SOC 2 Type 1 examination — target Q4 2026.
- SOC 2 Type 2 examination — target Q3 2027.
- PAnalytics quarterly recovery test and RTO/RPO documentation — available on request.
- Organization-wide penetration test — roadmap 2027.
- Microsoft Intune and Defender for Endpoint — phased deployment through 2026.