Trust Services Criteria (TSC) Mapping

Powered by AiVRIC

Purpose

This document provides a structured mapping between the **AICPA Trust Services Criteria (TSC)** and the controls, evidence, and continuous monitoring capabilities delivered by **AiVRIC**.

It is intended to support:

- SOC 2 Type I readiness
- SOC 2 Type II continuous monitoring
- Auditor walkthroughs and evidence validation
- Ongoing governance and control maturity tracking

Unlike static spreadsheets, this mapping reflects a **living control framework**, continuously validated through AiVRIC's automated scanning, findings, and dashboards.

How to Use This Document

- Each Trust Services Criterion includes:
  - **Control Objective**
  - **Points of Focus**
  - **Implementation Examples**
  - **Audit Evidence**
  - **AiVRIC Enablement**
- Controls may be:
  - ✅ Automated and continuously monitored by AiVRIC
  - ⚠️ Partially automated with supporting process evidence
  - ❌ Manual / process-based

This document should be reviewed **quarterly** and updated as systems, risk posture, or scope change.

Trust Services Categories Covered

- **Common Criteria (CC)** — Required for all SOC 2 reports
- **Availability (A)**
- **Confidentiality (C)**
- **Processing Integrity (PI)**
- **Privacy (P)**

COMMON CRITERIA (CC)

CC1.1 – Control Environment

Control Objective
The entity demonstrates a commitment to integrity and ethical values.

Points of Focus

- Tone at the top
- Standards of conduct
- Adherence monitoring
- Timely remediation of violations

Implementation Examples

- Documented Code of Conduct
- Annual ethics and security training
- Anonymous reporting mechanisms
- Disciplinary process enforcement

Evidence Required

- Code of Conduct
- Training completion records
- Ethics committee minutes
- Incident and disciplinary documentation

✅ **AiVRIC Enablement**

- Supports risk awareness inputs

- Provides technical risk data to governance reviews

CC1.2 – Board Independence & Oversight

Control Objective
The board provides independent oversight of the system of internal control.

Points of Focus

- Defined oversight responsibilities
- Relevant expertise
- Independent operation
- Review of control effectiveness

Implementation Examples

- Board-level security briefings
- Risk or audit committee oversight
- Formal review of security posture

Evidence Required

- Board and committee meeting minutes
- Security briefing decks
- Governance charters

✅ **AiVRIC Enablement**

- Supplies executive-level dashboards
- Produces evidence used in board reporting

CC1.3 – Organizational Structure & Authority

Control Objective
Management establishes reporting lines, authorities, and responsibilities.

Points of Focus

- Defined reporting structures

- Clear assignment of duties
- Escalation procedures

Implementation Examples

- Organizational charts
- RACI matrix
- Defined CISO and security roles

Evidence Required

- Org charts
- Job descriptions
- Responsibility matrices

✅ **AiVRIC Enablement**

- Aligns technical ownership with findings and remediation accountability

---

CC3.4 – Logical & Physical Access Controls

Control Objective
Access to systems and data is restricted based on risk and authorization.

Points of Focus

- User authentication
- Network segmentation
- Logical and physical access management
- Protection of information assets

Implementation Examples

- MFA enforcement
- RBAC and PAM
- Network segmentation
- Encryption at rest and in transit
- Badge-based facility access

Evidence Required

- Access control policies
- Access reviews
- MFA and encryption configurations
- Facility access logs

✅ **AiVRIC Enablement**

- Detects missing MFA
- Identifies over-privileged access
- Validates encryption and exposure risks

CC6.1 – Ongoing & Separate Evaluations

Control Objective
Controls are evaluated continuously and independently.

Points of Focus

- Rate of change
- Baseline understanding
- Skilled evaluators
- Integration with operations

Implementation Examples

- Continuous monitoring
- Internal audits
- Vulnerability scanning
- Penetration testing

Evidence Required

- Scan reports
- Audit reports
- Monitoring dashboards

✅ **AiVRIC Enablement**

- Core strength of AiVRIC
- Provides continuous control validation and historical evidence for Type II audits

CC7.1 – System Operations Monitoring

Control Objective
Security events and anomalies are detected and monitored.

Points of Focus

- Configuration standards
- Change detection
- Software monitoring
- Alerting mechanisms

Implementation Examples

- SIEM deployment
- IDS/IPS
- File integrity monitoring
- 24/7 alerting

Evidence Required

- SIEM logs
- Alert configurations
- Monitoring reports

✅ **AiVRIC Enablement**

- Validates monitoring coverage
- Identifies gaps in visibility and detection

CC7.2 – Incident Response

Control Objective
Security incidents are detected, contained, and resolved.

Points of Focus

- Assigned roles

- Incident containment
- Recovery processes

Implementation Examples

- IR plan and playbooks
- Ticketing system
- Tabletop exercises

Evidence Required

- Incident tickets
- IR documentation
- Exercise results

✅ **AiVRIC Enablement**

- Provides early detection signals
- Supports investigation evidence

CC7.3 – Vulnerability Management

Control Objective
Vulnerabilities are identified and remediated timely.

Points of Focus

- Change identification
- Risk assessment
- Remediation tracking

Implementation Examples

- Automated vulnerability scans
- Patch SLAs
- Risk acceptance documentation

Evidence Required

- Scan results
- Patch logs

- Remediation tracking

✅ **AiVRIC Enablement**

- Continuous vulnerability discovery
- Historical remediation evidence

AVAILABILITY (A)

A1.1 – System Availability

- SLA definition
- Uptime monitoring
- High-availability architecture

✅ **AiVRIC Enablement**

- Surfaces availability-impacting misconfigurations

A1.2 – Capacity & Infrastructure

- Capacity planning
- Redundancy
- Environmental monitoring

✅ **AiVRIC Enablement**

- Identifies single points of failure and misconfigurations

A1.3 – Backup & Recovery

- Backups
- DR plans
- Restoration testing

✅ **AiVRIC Enablement**

- Validates backup configurations and exposure risks

CONFIDENTIALITY (C)

C1.1 – Confidential Information Protection

C1.2 – Confidential Information Access

✅ **AiVRIC Enablement**

- Detects exposed storage
- Identifies weak data access controls

PROCESSING INTEGRITY (PI)

PI1.1 – PI1.3 – Data Processing & Error Management

✅ **AiVRIC Enablement**

- Supports integrity validation through configuration and exposure scanning

---

PRIVACY (P)

P1.1 – Notice

P2.1 – Consent

P4.1 – Retention

P5.1 – Data Access

✅ **AiVRIC Enablement**

- Supports system-level validation
- Complements privacy workflows and records

Continuous Compliance Advantage with AiVRIC

AiVRIC transforms SOC 2 from:

Annual audit preparation → Continuous trust validation

Benefits include:

- Real-time control visibility
- Evidence retention across audit periods
- Reduced audit fatigue
- Stronger Type II outcomes

Document Status

Review Cadence: Quarterly
Owner: Security & Compliance
Last Updated: _____
SOC 2 Scope: Type I ☐ Type II ☐