SOC 2 Readiness Workbook

Powered by AiVRIC

Purpose

This SOC 2 Readiness Workbook is designed to help organizations prepare for **SOC 2 Type I and Type II audits** by providing a structured, actionable framework aligned to the **AICPA Trust Services Criteria (TSC)**.

When paired with **AiVRIC continuous scanning and control visibility**, this workbook enables organizations to transition from checklist-based compliance to **continuous readiness and monitoring**.

How to Use This Workbook

- Treat this document as a **living readiness tracker**, not a one-time checklist
- Each section represents a **control domain aligned to SOC 2**
- Items should be marked as:
  - ✅ Implemented
  - ⚠️ In Progress
  - ❌ Not Started
- Evidence produced by **AiVRIC scans, findings, and dashboards** should be linked wherever applicable

---

Trust Services Categories Overview

SOC 2 is organized around five Trust Services Categories:

1. **Security** (Required)
2. **Availability** (Optional)
3. **Confidentiality** (Optional)
4. **Processing Integrity** (Optional)

5. **Privacy** (Optional)

✅ **Security is mandatory** for all SOC 2 reports
➕ Other categories are included based on customer, regulatory, or business requirements

---

SOC 2 Audit Types

- **Type I:**
  Evaluates whether controls are **designed effectively** at a specific point in time.
- **Type II:**
  Evaluates whether controls are **operating effectively over time** (typically 6–12 months).

AiVRIC strongly supports **Type II readiness** through continuous monitoring, historical scan evidence, and drift detection.

SECTION 1: SECURITY (Required)

1. Governance & Risk Assessment

Objective: Establish oversight, accountability, and risk awareness.

Task	Priority	Notes / Evidence
Document security org structure & reporting	High	Org chart, policies
Perform enterprise-wide risk assessment	High	Risk register
Create risk treatment plan	High	Mitigation plan
Establish security steering committee	Medium	Meeting records
Define RACI for security roles	Medium	Responsibility matrix

✅ **AiVRIC Support:**

- Identifies risk concentration areas
- Provides evidence for technical risk inputs

---

2. Policies & Procedures

Objective: Define formalized security expectations.

Required artifacts:

- Information Security Policy
- Acceptable Use Policy
- Access Control Policy
- Incident Response Policy
- Change Management Policy
- Vendor Management Policy
- Data Classification Policy
- BCDR Plan

✅ **AiVRIC Support:**

- Validates alignment between policy intent and technical enforcement
- Highlights gaps via findings (e.g., logging, encryption, IAM)

---

3. Access Controls

Objective: Enforce least privilege and secure identity management.

Control	Priority
MFA across systems	High
SSO implementation	High
RBAC enforcement	High
User provisioning & deprovisioning	High
Quarterly access reviews	High
Privileged access management	High

✅ **AiVRIC Support:**

- Detects missing MFA
- Identifies over-privileged roles
- Flags dormant accounts

---

4. Security Monitoring & Logging

Objective: Detect and respond to security events.

Key requirements:

- Centralized logging (SIEM)
- 90+ day log retention
- Real-time alerts
- Audit logs enabled

✅ **AiVRIC Support:**

- Validates logging configurations
- Confirms audit logging coverage
- Supports CC7.x monitoring controls

---

5. Vulnerability & Patch Management

Objective: Identify and remediate technical weaknesses.

Requirement	Priority
Automated vulnerability scanning	High
Patch management SLAs	High
CI/CD security testing	Medium
Periodic penetration testing	Medium

✅ **AiVRIC Support:**

- Continuous vulnerability & misconfiguration scanning
- Historical findings for audit evidence

---

6. Encryption & Data Protection

Objective: Protect data confidentiality and integrity.

- Encryption at rest
- Encryption in transit (TLS 1.2+)
- Key management
- Encrypted backups

✅ **AiVRIC Support:**

- Identifies unencrypted storage
- Flags weak transport configurations

---

7. Physical & Environmental Security

Objective: Protect facilities and infrastructure.

- Cloud provider SOC reports
- Office access controls
- Visitor procedures
- Environmental safeguards

✅ **AiVRIC Support:**

- Indirect (cloud provider attestation evidence)

---

8. Incident Response

Objective: Detect, respond, and recover from incidents.

Control	Priority
IR team & roles defined	High
IR playbooks	High
Escalation procedures	High
Tabletop exercises	Medium
Incident tracking	Medium

✅ **AiVRIC Support:**

- Provides detection signals
- Supplies evidence of ongoing monitoring

---

9. Training & Awareness

Objective: Reduce human risk.

- Annual security training
- Phishing simulations
- Secure coding education
- Training completion tracking

✅ **AiVRIC Support:**

- Validates enforcement-side readiness
- Complements training records

---

10. Vendor Management

Objective: Manage third-party risk.

Requirement	Priority
Vendor inventory	High
Vendor assessments	High
SOC 2 reviews	High
Ongoing vendor risk monitoring	Medium

✅ **AiVRIC Support:**

- Identifies external exposure and integrations
- Supports vendor risk visibility

OPTIONAL CATEGORIES (AS APPLICABLE)

Availability

- SLAs & uptime targets
- Monitoring & alerting
- Redundancy & failover
- BCDR testing

Confidentiality

- Data classification
- DLP controls
- NDA management

Processing Integrity

- Secure SDLC
- Change validation
- Data integrity monitoring

Privacy

- Privacy policy
- Consent management
- DSAR procedures
- Data sharing & DPAs

Continuous Monitoring with AiVRIC

AiVRIC transforms SOC 2 from a one-time project into an **ongoing operational program** by providing:

- Continuous control validation
- Historical evidence for Type II audits
- Control drift detection
- Executive and auditor-ready reporting

Readiness Completion Checklist

✅ All required Security controls implemented
✅ Optional categories scoped and addressed
✅ High & critical findings remediated or accepted
✅ Evidence collected and exported
✅ Management review completed

SOC 2 Readiness Status: ☐ Ready ☐ In Progress ☐ Not Ready

Summary

This workbook, combined with AiVRIC's continuous scanning and visibility, provides a **clear, defensible path to SOC 2 readiness**—reducing manual effort, improving audit outcomes, and enabling sustained compliance beyond certification.