SOC 2 Readiness Checklist

20 Things Auditors Look For — Before You Schedule Your Audit

CMMC | NIST 800-171 | SOC 2 | Risk Advisory

PeakVisibility Partners
peakvisibilitypartners.com
Veteran-Owned Small Business

Use this checklist to assess where your company stands before starting your SOC 2 journey. Each item maps directly to what auditors evaluate. Check off what you have in place — gaps are where you'll focus your readiness program.

■ POLICIES & DOCUMENTATION — 4 ITEMS

- ☐ **01 Information Security Policy**
  A documented, board-approved security policy that defines your security objectives, scope, roles and responsibilities, and commitment to protecting customer data.
- ☐ **02 Acceptable Use Policy**
  Written rules governing how employees, contractors, and vendors may use company systems, data, and networks — signed by all personnel.
- ☐ **03 Incident Response Plan**
  A documented procedure for detecting, responding to, and recovering from security incidents — including defined escalation paths and notification timelines.
- ☐ **04 Vendor / Third-Party Risk Policy**
  A process for assessing security posture of vendors who access your systems or handle customer data, including contract requirements and periodic reviews.

■ ACCESS CONTROL — 4 ITEMS

- ☐ **05 Role-Based Access Control (RBAC)**
  Users are granted only the minimum access needed to perform their job. Access is defined by role, not individual, and reviewed at least quarterly.
- ☐ **06 Multi-Factor Authentication (MFA)**
  MFA is enforced for all users accessing production systems, cloud environments, and any system storing or processing customer data.
- ☐ **07 Access Review & Deprovisioning**
  Formal process to review user access rights periodically and immediately revoke access when employees leave or change roles — with documented evidence.
- ☐ **08 Privileged Access Management**
  Admin and elevated accounts are tracked, require approval for use, and activity is logged. Shared credentials are not used for privileged access.

■■ RISK MANAGEMENT — 3 ITEMS

- [ ] **09** **Formal Risk Assessment Process**
  A documented, recurring risk assessment identifies threats, vulnerabilities, and likelihood/impact ratings — with a risk register updated at least annually.

- [ ] **10** **Risk Treatment & Remediation Tracking**
  Identified risks have assigned owners, remediation plans, target dates, and documented evidence of resolution or accepted risk with leadership sign-off.

- [ ] **11** **Business Continuity & Disaster Recovery Plan**
  Documented BCP/DRP defines recovery time objectives (RTO), recovery point objectives (RPO), and has been tested within the last 12 months.

■ MONITORING & LOGGING — 3 ITEMS

- [ ] **12** **Centralized Log Management**
  Security-relevant logs (authentication, access, system events) are collected centrally, retained for a defined period, and protected from tampering.

- [ ] **13** **Continuous Security Monitoring**
  Automated tools monitor for unauthorized access, anomalous activity, and security events — with alerts routed to responsible personnel for review.

- [ ] **14** **Vulnerability Management Program**
  Regular vulnerability scans are conducted, results are reviewed and prioritized, and critical findings are remediated within defined SLAs with documented evidence.

■■ CHANGE MANAGEMENT & DEVELOPMENT — 3 ITEMS

- [ ] **15** **Change Management Process**
  All changes to production systems follow a documented approval workflow — including testing, rollback plans, and audit logs of who approved and deployed.

- [ ] **16** **Secure Development Practices**
  Developers follow documented secure coding standards, code reviews include security checks, and dependency/vulnerability scanning is part of the CI/CD pipeline.

- [ ] **17** **Separation of Environments**
  Development, staging, and production environments are logically or physically separated. Production data is not used in development or testing.

■ AVAILABILITY & ENCRYPTION — 3 ITEMS

☐ **18** **Data Encryption at Rest and in Transit**
All customer data is encrypted at rest (AES-256 or equivalent) and in transit (TLS 1.2+). Encryption key management is documented and keys are rotated on schedule.

☐ **19** **Backup & Recovery Testing**
Data backups are automated, encrypted, stored separately from primary systems, and restoration is tested and documented at least annually.

☐ **20** **Uptime & Availability Monitoring**
System availability is measured against defined SLAs, monitored continuously, and incidents affecting availability are logged, escalated, and reviewed.

SCORE YOUR READINESS

0–6 Checked	7–12 Checked	13–17 Checked	18–20 Checked
HIGH RISK	**MODERATE RISK**	**LOW RISK**	**AUDIT READY**
Significant gaps. Enterprise deals will stall. Start readiness immediately.	Foundational controls exist but evidence and documentation need work.	Good posture. Focus on evidence collection and audit coordination.	Strong controls in place. Schedule your Type I audit with confidence.

Not Sure Where You Stand?

Book a free 15-minute SOC 2 Readiness Call with our team. We'll review your checklist, identify your biggest gaps, and give you a clear path to audit-ready — no obligation.

www.peakvisibilitypartners.com
admin@peakvisibilitypartners.com | (980) 221-0943