SOC 2 Provider Due-Diligence Checklist

Evaluate auditor qualifications, independence, provider relationships and examination quality.

HOW TO USE Complete before signing an engagement letter. Retain written answers and supporting documentation.

1. Identify the responsible CPA firm

- ☐ Legal name of the CPA firm that will issue and sign the SOC report
- ☐ Name and credentials of the engagement partner
- ☐ State(s) in which the firm and practitioner are licensed
- ☐ License verified through the applicable state board of accountancy
- ☐ CPA firm - not only the platform - is clearly named in the proposal and engagement letter

2. Verify quality oversight and experience

- ☐ Firm confirms enrollment in an AICPA-approved peer-review program
- ☐ Firm explains whether SOC engagements are included in its practice subject to peer review
- ☐ Team has relevant SOC 1/SOC 2 and industry experience
- ☐ Proposal identifies engagement review and quality-control responsibilities
- ☐ References or representative experience have been evaluated

3. Understand business relationships

- ☐ All referral fees, revenue shares, commissions or marketplace-placement fees are disclosed
- ☐ Ownership, investment or other financial relationships are disclosed
- ☐ Auditor explains how threats to independence and objectivity were evaluated
- ☐ Auditor is free to report exceptions without pressure from a platform or readiness provider
- ☐ No contract term appears to condition compensation on a clean or favorable report

4. Separate management, readiness and audit roles

- ☐ Management retains responsibility for controls, the system description and assertions
- ☐ Readiness provider does not make management decisions
- ☐ Auditor does not design controls and then audit its own work without an appropriate independence analysis
- ☐ Platform supports workflow but does not replace auditor judgment
- ☐ Roles are documented in proposals and engagement letters

5. Evaluate the proposed examination

- ☐ Report type, Trust Services Categories, system boundaries and period are defined
- ☐ Locations, subservice organizations, vendors and complementary controls are addressed
- ☐ Testing includes procedures appropriate to each control - not only automated status checks
- ☐ Auditor explains how evidence reliability and contradictory information are evaluated
- ☐ Timeline allows for planning, testing, exception follow-up, review and reporting

6. Test the promises and pricing

- ☐ Provider does not guarantee a clean report or use certification language inaccurately
- ☐ Fee is consistent with scope, complexity and examination period
- ☐ Change-order triggers and out-of-scope work are explained
- ☐ Management understands what the platform fee includes versus the CPA firm fee
- ☐ Renewal terms, data access and evidence-export rights are clear

7. Confirm reporting and follow-up

- ☐ Process for communicating exceptions is defined
- ☐ Management representation responsibilities are explained
- ☐ Draft-review boundaries do not permit management to suppress valid findings
- ☐ Final report distribution and restricted-use requirements are explained
- ☐ Plan addresses bridge letters, annual renewal and remediation follow-up

Selection decision

Decision	Select a decision		
Provider selected			
Decision owner		**Date**	
Unresolved concerns			
Safeguards / follow-up			

This practical screening tool is not a substitute for legal or professional advice. Independence conclusions depend on the facts, applicable professional rules and services involved.

Learn more about JConner's SOC readiness and examination services at www.jconnerpc.com.