SOC 2 Vendor Questions

Interview Worksheet

Plow Networks

Prepared 2026

7101 Sharondale Court
Suite 200
Brentwood, TN 37027
plow.net

Use this worksheet during vendor calls or security questionnaire review. Record responses and flag concerns for follow-up. Green indicators suggest maturity; red flags warrant deeper investigation.

Field	Value
Vendor:	
Date:	
Interviewer:	

Question 1: Report Availability & Type

Ask: "Do you have a current SOC 2 report? Is it Type 1 or Type 2?"

Good Answer Indicators	Red Flags
• Type 2 report available • Report issued within last 12 months • 12-month observation period • Offers to share under NDA	• Only Type 1 with no Type 2 timeline • Report is over 18 months old • "Working on it" for years • Refuses to share or can't locate

Vendor Response: _____

Question 2: Trust Service Criteria Coverage

Ask: "Which Trust Service Criteria does your SOC 2 report cover, and why did you select those?"

Good Answer Indicators	Red Flags
• Clear explanation of criteria selected • Rationale tied to business/service type • Includes criteria relevant to your use • Security + applicable optional criteria	• Doesn't know what criteria are covered • Security-only with no explanation • Missing criteria you need (Privacy, etc.) • Defensive about scope limitations

Vendor Response: _____

Question 3: Audit Scope & Services

Ask: "Does your SOC 2 audit scope include the specific products and services we're purchasing?"

Good Answer Indicators	Red Flags
• Confirms specific services in scope • Points to system description section • Explains what's included vs. excluded • Recent acquisitions integrated	• Unsure if your services are covered • Recent acquisitions not yet in scope • Scope only covers legacy products • Infrastructure you use is carved out

Vendor Response: _____

Question 4: Exceptions & Remediation

Ask: "Were there any exceptions in your most recent report? How were they addressed?"

Good Answer Indicators	Red Flags
• Transparent about any exceptions • Clear remediation plan with timeline • Can show evidence of fixes • Exceptions not in critical control areas	• Claims "no exceptions ever" • Same exceptions year after year • Exceptions in access/data controls • Defensive or dismissive response

Vendor Response: _____

Question 5: Continuous Monitoring

Ask: "What happens between audit cycles? How do you maintain controls year-round?"

Good Answer Indicators	Red Flags
• Continuous monitoring in place • Regular internal audits/reviews • Automated control testing • Dedicated compliance/security team	• "We wait for the next audit" • No ongoing monitoring described • Compliance treated as annual event • No dedicated compliance resources

Vendor Response: _____

Question 6: Subservice Organizations

Ask: "Do you use any third-party subservice organizations? Are they included in your SOC 2 scope?"

Good Answer Indicators	Red Flags
• Clear list of subservice orgs • Inclusive method (included in scope) • Or carve-out with own SOC 2s • Complementary user entity controls	• Doesn't know subservice orgs used • Major dependencies carved out • Carved out with no SOC 2 evidence • Unclear about third-party controls

Vendor Response: _____

Assessment Summary

Metric	Value
Total Good Indicators:	_____ / 24
Total Red Flags:	_____ / 24
Overall Impression:	☐ Proceed ☐ Follow-up Needed ☐ Concerns

Key Concerns to Address: _____

Follow-up Actions: _____