SOC-2 Gap Analysis Worksheet

A practical tool for assessing your SOC-2 readiness

How to Use This Worksheet

This worksheet helps you assess your current security posture against the **9 Common Criteria (CC1–CC9)** required for SOC-2.

■ **Estimated time:** 30–45 minutes

■ **Who should complete:** Founder, CTO, or lead engineer

Company Information

Field	Your Answer
Company Name	
Primary Contact	
Number of Employees	
Core Product / Service	
Target Audit Timeline	■ 3 months ■ 6 months ■ 1 year ■ Just exploring
Desired Trust Services Criteria	■ Security (mandatory) ■ Confidentiality ■ Availability ■ Processing Integrity ■ Privacy

What happens after: You'll have a clear view of your gaps and can prioritize next steps.

CC1: Control Environment

The foundation of your security program — policies, roles, and accountability.

Key Questions	Your Status
Do you have a formal Information Security Policy?	■ Yes ■ No ■ Partial
Has leadership formally assigned security responsibilities?	■ Yes ■ No ■ Partial
Do employees receive security training?	■ Yes ■ No ■ Partial

Evidence to look for: Written policy, job descriptions, training records

Gap Severity: ■ High ■ Medium ■ Low

Notes: _____

CC2: Communication and Information

How security expectations are communicated internally.

Key Questions	Your Status
Are security policies accessible to all employees?	■ Yes ■ No ■ Partial
Is there a process for reporting security concerns?	■ Yes ■ No ■ Partial
Do employees acknowledge policies?	■ Yes ■ No ■ Partial

Evidence to look for: Policy acknowledgments, reporting channels (e.g., email, Slack)

Gap Severity: ■ High ■ Medium ■ Low

Notes: _____

CC3: Risk Assessment

Identifying and managing security risks.

Key Questions	Your Status
Have you performed a formal risk assessment?	■ Yes ■ No ■ Partial
Is risk assessment repeated annually?	■ Yes ■ No ■ Partial
Are risks documented and tracked?	■ Yes ■ No ■ Partial

Evidence to look for: Risk register, assessment report, remediation plan

Gap Severity: ■ High ■ Medium ■ Low

Notes: _____

CC4: Monitoring Activities

Tracking whether controls are working.

Key Questions	Your Status
Do you monitor security controls for effectiveness?	■ Yes ■ No ■ Partial
Are exceptions documented and addressed?	■ Yes ■ No ■ Partial
Do you have a process for control failures?	■ Yes ■ No ■ Partial

Evidence to look for: Monitoring logs, exception reports, remediation tickets

Gap Severity: ■ High ■ Medium ■ Low

Notes: _____

CC5: Control Activities

The specific controls you have in place.

Key Questions	Your Status
Are controls documented and designed to address risks?	■ Yes ■ No ■ Partial
Are controls operating effectively?	■ Yes ■ No ■ Partial
Are control changes reviewed?	■ Yes ■ No ■ Partial

Evidence to look for: Control descriptions, evidence of operation, change logs

Gap Severity: ■ High ■ Medium ■ Low

Notes: _____

CC6: Logical and Physical Access Controls

Who can access what, and how.

Key Questions	Your Status
Is MFA required for all remote access?	■ Yes ■ No ■ Partial
Are access reviews performed quarterly?	■ Yes ■ No ■ Partial
Is access removed within 24 hours of termination?	■ Yes ■ No ■ Partial
Are privileged accounts restricted?	■ Yes ■ No ■ Partial

Evidence to look for: MFA configuration, access review records, termination procedures

Gap Severity: ■ High ■ Medium ■ Low

Notes: _____

CC7: System Operations

How systems are monitored and protected.

Key Questions	Your Status
Do you have an Incident Response Plan?	■ Yes ■ No ■ Partial
Has the Incident Response Plan been tested?	■ Yes ■ No ■ Partial
Do you monitor for security events?	■ Yes ■ No ■ Partial
Are vulnerabilities scanned regularly?	■ Yes ■ No ■ Partial

Evidence to look for: IR plan, test results, monitoring dashboards, scan reports

Gap Severity: ■ High ■ Medium ■ Low

Notes: _____

CC8: Change Management

How changes to systems are controlled.

Key Questions	Your Status
Is there a formal change approval process?	■ Yes ■ No ■ Partial
Are changes tested before deployment?	■ Yes ■ No ■ Partial
Are emergency changes documented?	■ Yes ■ No ■ Partial

Evidence to look for: Change tickets, approval records, test results

Gap Severity: ■ High ■ Medium ■ Low

Notes: _____

CC9: Risk Mitigation

Managing vendor and business continuity risks.

Key Questions	Your Status
Do you assess third-party vendors?	■ Yes ■ No ■ Partial
Do you have a business continuity plan?	■ Yes ■ No ■ Partial
Is backup and recovery tested?	■ Yes ■ No ■ Partial

Evidence to look for: Vendor assessments, BC plan, backup test results

Gap Severity: ■ High ■ Medium ■ Low

Notes: _____

Summary & Prioritization

Priority Level	Count	Examples / Notes
High — Must fix immediately		
Medium — Fix before audit		
Low — Can phase in		
✓ Already Compliant		

Top 5 Recommended Actions

1. _____
2. _____
3. _____
4. _____
5. _____

Next Steps

- Share this worksheet with your team
- Schedule a follow-up call with Audit Vault to review results
- Begin implementing high-priority fixes

Need help? Book a free strategy call: **hello@auditvault.org**