

# SOC 2

## Compliance Assessment Questionnaire

---

46 Assessment Questions • 13 Control Domains

### ORGANIZATION INFORMATION

Organization Name:

-----

Assessment Date:

-----

Assessor Name / Title:

-----

System / Scope:

-----

### SCORING METHOD

- YES** (2 points) — Fully implemented — control is in place, documented, and operating effectively.
- PARTIAL** (1 point) — Partially implemented — some elements are in place but gaps remain.
- NO** (0 points) — Not implemented — control is missing or not operating.

**Compliance Score = (Total Points ÷ Maximum Points) × 100%**

Maximum possible points: 92 (46 questions × 2 points each)

# CC1 — CONTROL ENVIRONMENT (COSO)

Reference: CC1

**Q1** [CC1.1]

## Does the organization demonstrate a commitment to integrity and ethical values?

*Auditors expect to see a code of conduct, ethics policies, and evidence of communication and enforcement. Collect documentation of policies, training records, and disciplinary actions to assess both design and operational effectiveness.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

**Q2** [CC1.2]

## Is there a board of directors or equivalent oversight body that exercises oversight of the development and performance of internal control?

*Auditors look for board charters, meeting minutes, and oversight reports. Evidence should include documentation of board activities and their involvement in internal control matters.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

**Q3** [CC1.3]

## Does management establish, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities?

*Auditors expect organizational charts, job descriptions, and delegation of authority documents. Collect these records to evaluate the design and effectiveness of the control environment.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

**Q4** [CC1.4]

## Does the organization demonstrate a commitment to attract, develop, and retain competent individuals?

*Auditors look for hiring policies, training programs, and performance evaluations. Evidence should include HR policies, training records, and appraisal documents.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

**Q5** [CC1.5]

## Does the organization hold individuals accountable for their internal control responsibilities?

*Auditors expect performance reviews, accountability policies, and records of corrective actions. Collect documentation that demonstrates accountability mechanisms are in place and functioning.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

## CC2 — COMMUNICATION AND INFORMATION

Reference: CC2

---

**Q6** [CC2.1]

**Does the organization obtain or generate and use relevant, quality information to support the functioning of internal control?**

*Auditors look for information management policies, data quality assessments, and examples of information used in decision-making. Evidence should demonstrate that information is accurate, timely, and relevant.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q7** [CC2.2]

**Does the organization internally communicate information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control?**

*Auditors expect internal communication policies, meeting minutes, and internal memos. Collect evidence showing that critical information is effectively communicated within the organization.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q8** [CC2.3]

**Does the organization communicate with external parties regarding matters affecting the functioning of internal control?**

*Auditors look for communication policies with external stakeholders, records of external communications, and feedback mechanisms. Evidence should demonstrate that relevant information is shared appropriately with external parties.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

## CC3 — RISK ASSESSMENT

Reference: CC3

---

**Q9** [CC3.1]

**Does the organization specify objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives?**

*Auditors expect documented objectives, risk assessment processes, and risk registers. Collect evidence that objectives are clearly defined and risks are identified and assessed in relation to these objectives.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q10** [CC3.2]

**Does the organization identify risks to the achievement of its objectives across the entity and analyze risks as a basis for determining how the risks should be managed?**

*Auditors look for risk identification methodologies, risk assessments, and risk treatment plans. Evidence should demonstrate a systematic approach to identifying and analyzing risks.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q11** [CC3.3]

**Does the organization consider the potential for fraud in assessing risks to the achievement of objectives?**

*Auditors expect fraud risk assessments, anti-fraud policies, and records of fraud detection activities. Collect evidence that the organization proactively considers and addresses fraud risks.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q12** [CC3.4]

**Does the organization identify and assess changes that could significantly impact the system of internal control?**

*Auditors look for change management policies, records of significant changes, and impact assessments. Evidence should show that changes are evaluated for their impact on internal controls.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

## CC4 — MONITORING ACTIVITIES

Reference: CC4

---

**Q13** [CC4.1]

**Does the organization select, develop, and perform ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning?**

*Auditors expect internal audit reports, self-assessment records, and evaluation plans. Collect evidence that monitoring activities are designed and implemented effectively.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q14** [CC4.2]

**Does the organization evaluate and communicate internal control deficiencies in a timely manner to those parties responsible for taking corrective action?**

*Auditors look for deficiency reports, communication records, and corrective action plans. Evidence should demonstrate that deficiencies are identified, communicated, and addressed promptly.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

## CC5 — CONTROL ACTIVITIES

Reference: CC5

---

**Q15** [CC5.1]

**Does the organization select and develop control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels?**

*Auditors expect risk control matrices, control design documents, and implementation records. Collect evidence that control activities are appropriately designed to mitigate identified risks.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q16** [CC5.2]

**Does the organization select and develop general control activities over technology to support the achievement of objectives?**

*Auditors look for IT control frameworks, system control policies, and implementation evidence. Evidence should demonstrate that technology controls are in place and support organizational objectives.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q17** [CC5.3]

**Does the organization deploy control activities through policies that establish what is expected and procedures that put policies into action?**

*Auditors expect policy documents, procedure manuals, and records of policy enforcement. Collect evidence that policies are clearly defined and effectively implemented through procedures.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

# CC6 — LOGICAL AND PHYSICAL ACCESS CONTROLS

Reference: CC6

**Q18** [CC6.1]

**Does the organization implement logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives?**

*Auditors look for access control policies, system architecture diagrams, and access logs. Evidence should demonstrate that logical access controls are effectively designed and implemented.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

**Q19** [CC6.2]

**Does the organization implement physical access security measures to protect information assets from security events to meet the entity’s objectives?**

*Auditors expect physical security policies, access control records, and surveillance logs. Collect evidence that physical access controls are in place and functioning as intended.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

**Q20** [CC6.3]

**Does the organization implement controls to restrict the transmission, movement, and removal of information to authorized internal and external users and processes?**

*Auditors look for data transfer policies, encryption protocols, and transfer logs. Evidence should demonstrate that data movement is controlled and restricted to authorized entities.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

**Q21** [CC6.4]

**Does the organization implement controls to protect against external threats?**

*Auditors expect threat management policies, intrusion detection system logs, and incident response records. Collect evidence that external threats are identified and mitigated effectively.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

# CC7 — SYSTEM OPERATIONS

Reference: CC7

---

**Q22** [CC7.1]

**Does the organization implement detection and monitoring procedures to identify changes to configurations that may diminish the security posture?**

*Auditors look for monitoring policies, configuration management records, and change detection logs. Evidence should demonstrate that system configurations are monitored for unauthorized changes.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q23** [CC7.2]

**Does the organization monitor system components and the operation of those components for anomalies indicative of malicious acts, natural disasters, and errors?**

*Auditors expect system monitoring policies, anomaly detection logs, and incident reports. Collect evidence that system operations are monitored for unusual activities and potential threats.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q24** [CC7.3]

**Does the organization evaluate security events to determine their nature and assess whether they represent security incidents?**

*Auditors look for incident response policies, event analysis records, and incident classification procedures. Evidence should demonstrate that security events are evaluated and classified appropriately.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q25** [CC7.4]

**Does the organization respond to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate?**

*Auditors expect incident response plans, incident logs, and post-incident analysis reports. Collect evidence that security incidents are managed according to a defined response program.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q26** [CC7.5]

**Does the organization identify, develop, and implement activities to recover from identified security incidents?**

*Auditors look for recovery plans, backup records, and system restoration logs. Evidence should demonstrate that recovery activities are planned and executed effectively following security incidents.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

## CC8 — CHANGE MANAGEMENT

Reference: CC8

---

**Q27** [CC8.1]

**Does the organization manage changes to system components to meet the entity's objectives?**

*Auditors expect change management policies, change request records, and approval logs. Collect evidence that changes are managed systematically to maintain system integrity and security.*

**YES**

**PARTIAL**

**NO**

Explanation: \_\_\_\_\_

---

---

## CC9 — RISK MITIGATION

Reference: CC9

---

**Q28** [CC9.1]

**Does the organization identify, select, and develop risk mitigation activities for risks arising from potential business disruptions?**

*Auditors look for business continuity plans, risk assessments, and mitigation strategies. Evidence should demonstrate that risks are identified and mitigated to ensure business continuity.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q29** [CC9.2]

**Does the organization identify, select, and develop risk mitigation activities for risks arising from vendors and business partners?**

*Auditors expect vendor risk management policies, third-party assessments, and contract reviews. Collect evidence that risks from external parties are assessed and mitigated appropriately.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

# AVAILABILITY (A1)

Reference: A1

---

**Q30** [A1.1]

**Does the organization maintain and monitor system capacity to meet its objectives?**

*Auditors look for capacity planning documents, monitoring logs, and performance reports. Evidence should demonstrate that system capacity is managed to support availability commitments.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q31** [A1.2]

**Does the organization implement environmental protections to prevent and detect fires or other environmental threats?**

*Auditors expect environmental control policies, inspection records, and maintenance logs. Collect evidence that environmental threats are mitigated to ensure system availability.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q32** [A1.3]

**Does the organization implement data backup processes to support system recovery?**

*Auditors look for backup policies, backup schedules, and restoration test records. Evidence should demonstrate that data backups are performed and tested to support availability objectives.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q33** [A1.4]

**Does the organization implement recovery plan testing to ensure system availability objectives are met?**

*Auditors expect disaster recovery plans, test schedules, and test results. Collect evidence that recovery plans are tested to confirm their effectiveness in maintaining system availability.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

# PROCESSING INTEGRITY (PI1)

Reference: PI1

---

**Q34** [PI1.1]

## Does the organization define system processing integrity objectives to meet its commitments?

*Auditors look for documented processing objectives, system design documents, and validation records. Evidence should demonstrate that processing integrity objectives are clearly defined and implemented.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q35** [PI1.2]

## Does the organization implement procedures to prevent, detect, and correct processing errors?

*Auditors expect error handling policies, incident logs, and correction records. Collect evidence that processing errors are managed to maintain processing integrity.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q36** [PI1.3]

## Does the organization implement system inputs, processing, and outputs to meet processing integrity objectives?

*Auditors look for input validation procedures, processing controls, and output verification records. Evidence should demonstrate that system processes are designed to ensure processing integrity.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q37** [PI1.4]

## Does the organization implement data processing activities in accordance with defined processing integrity objectives?

*Auditors expect processing policies, operational records, and quality assurance reports. Collect evidence that data processing activities align with processing integrity objectives.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

# CONFIDENTIALITY (C1)

Reference: C1

---

**Q38** [C1.1]

**Does the organization identify and document confidential information to meet its objectives?**

*Auditors look for data classification policies, inventories of confidential information, and access control records. Evidence should demonstrate that confidential information is identified and managed appropriately.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q39** [C1.2]

**Does the organization implement controls to restrict access to confidential information to authorized personnel?**

*Auditors expect access control policies, user access lists, and audit logs. Collect evidence that access to confidential information is restricted and monitored.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q40** [C1.3]

**Does the organization implement procedures to protect confidential information from unauthorized disclosure?**

*Auditors look for data protection policies, encryption protocols, and incident response records. Evidence should demonstrate that confidential information is safeguarded against unauthorized disclosure.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

**Q41** [C1.4]

**Does the organization implement procedures to retain and dispose of confidential information in accordance with its objectives?**

*Auditors expect data retention policies, disposal procedures, and records of data destruction. Collect evidence that confidential information is retained and disposed of appropriately.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

# PRIVACY (P1)

Reference: P1

---

**Q42** [P1.1]

**Does the organization provide notice to data subjects about its privacy practices?**

*Auditors look for privacy policies, notices, and records of communication. Evidence should demonstrate that data subjects are informed about privacy practices.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q43** [P1.2]

**Does the organization obtain consent from data subjects for the collection, use, and disclosure of their personal information?**

*Auditors expect consent forms, records of consent, and procedures for obtaining consent. Collect evidence that consent is obtained and documented appropriately.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q44** [P1.3]

**Does the organization implement procedures to provide data subjects with access to their personal information?**

*Auditors look for access request procedures, records of access requests, and response logs. Evidence should demonstrate that data subjects can access their personal information as required.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q45** [P1.4]

**Does the organization implement procedures to correct or delete personal information upon request by data subjects?**

*Auditors expect correction and deletion procedures, records of requests, and action logs. Collect evidence that personal information is corrected or deleted in response to data subject requests.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

**Q46** [P1.5]

**Does the organization implement procedures to protect personal information from unauthorized access, use, or disclosure?**

*Auditors look for data protection policies, access controls, and incident response records. Evidence should demonstrate that personal information is safeguarded against unauthorized activities.*

YES

PARTIAL

NO

Explanation: \_\_\_\_\_

---

---

# COMPLIANCE SCORE SUMMARY

| Control Domain                             | Questions | Points Earned | Max Points | Score %      |
|--|-----------|---------------|------------|--------------|
| CC1 — Control Environment (COSO)           | 5         | ___           | 10         | ___ %        |
| CC2 — Communication and Information        | 3         | ___           | 6          | ___ %        |
| CC3 — Risk Assessment                      | 4         | ___           | 8          | ___ %        |
| CC4 — Monitoring Activities                | 2         | ___           | 4          | ___ %        |
| CC5 — Control Activities                   | 3         | ___           | 6          | ___ %        |
| CC6 — Logical and Physical Access Controls | 4         | ___           | 8          | ___ %        |
| CC7 — System Operations                    | 5         | ___           | 10         | ___ %        |
| CC8 — Change Management                    | 1         | ___           | 2          | ___ %        |
| CC9 — Risk Mitigation                      | 2         | ___           | 4          | ___ %        |
| Availability (A1)                          | 4         | ___           | 8          | ___ %        |
| Processing Integrity (PI1)                 | 4         | ___           | 8          | ___ %        |
| Confidentiality (C1)                       | 4         | ___           | 8          | ___ %        |
| Privacy (P1)                               | 5         | ___           | 10         | ___ %        |
| <b>TOTAL</b>                               | <b>46</b> | <b>___</b>    | <b>92</b>  | <b>___ %</b> |

## SCORE INTERPRETATION

- 90–100% — Strong Compliance**  
Organization demonstrates robust controls across all domains. Minor improvements may be needed.
- 70–89% — Moderate Compliance**  
Most controls are in place but notable gaps exist. Remediation plan recommended within 90 days.
- 50–69% — Partial Compliance**  
Significant gaps in compliance posture. Prioritized remediation required. Consider engaging a consultant.
- Below 50% — Non-Compliant**  
Organization does not meet minimum compliance requirements. Immediate action required.

---

## ATTESTATION

Assessed by: \_\_\_\_\_ Signature: \_\_\_\_\_  
Title: \_\_\_\_\_ Date: \_\_\_\_\_  
Reviewed by: \_\_\_\_\_ Signature: \_\_\_\_\_  
Title: \_\_\_\_\_ Date: \_\_\_\_\_

This assessment questionnaire was generated by whois-secure.com on May 23, 2026. It is provided for informational and self-assessment purposes only. This document does not constitute a formal compliance certification or audit. Organizations should engage a qualified assessor (C3PAO, CPA firm, or authorized auditor) for official compliance validation.