



SOC 2 Attestation Readiness Self-Assessment

The Next Layer of Trust



Your partner
in progress

Where does your organization stand on SOC 2 readiness?

Clients, partners and investors are increasingly asking service organizations to prove not just claim that customer data is properly protected. Whether that request comes from a contract requirement or a desire to stand out to global partners, the question is the same: are your controls ready to be examined by an independent CPA firm?

This self-assessment is designed to help you understand where your organization stands today, so you know what to prioritise before pursuing a formal SOC 2 examination.

Introducing SOC 2 Attestation

SOC 2 — SOC for Service Organizations: Trust Services Criteria is an examination engagement, performed in accordance with AICPA standards, that demonstrates how an organization's controls address criteria across up to five Trust Services Categories: Security (mandatory for all examinations), Availability, Processing Integrity, Confidentiality, and Privacy.

The examination is performed, and the report signed, by a licensed CPA firm. BSI coordinates the engagement end to end, working with a partner CPA firm that performs the examination and issues the SOC 2 report.

A SOC 2 examination can be Type 1 (control design at a point in time) or Type 2 (design and operating effectiveness over a period, typically 3–12 months).

A SOC 2 report is a restricted-use report: it is intended for customers and stakeholders with sufficient knowledge of the system, typically under a confidentiality agreement. For broader communication such as on a website, with partners, or with investors a SOC 3 general-use report can be issued based on the same examination.

SOC 2 is most valuable for organizations providing B2B services involving sensitive or personal data, particularly those serving US-based clients or operating in markets where clients require independent assurance of security controls.



Sections covered in this self-assessment

1. Scope, Client Requirements & Risk Context
2. Security (mandatory for all SOC 2 examinations)
3. Availability & Processing Integrity (optional selected based on service commitments)
4. Confidentiality & Privacy (optional selected based on service commitments)
5. Governance & Risk Management
6. Vendor & Third-Party Risk
7. Monitoring, Evidence & Examination Readiness

How the self-assessment works

Work through the checklist on the following pages. For each statement, mark Yes or No. Each ‘Yes’ counts as one point towards your final score. Once complete, use your score to identify your readiness stage and recommended next step.

Please answer based on your current state, not your aspirations — the value of this assessment is in an honest reflection of where you are today. This self-assessment is for guidance only and does not replace a formal SOC 2 readiness review.

Snapshot of our SOC 2 readiness scores

Early stage

0-10 Points

You’re at the start of your SOC 2 journey — the focus now is understanding scope and building foundational controls

Learn more >

Developing Stage

11-20 Points

Core controls are taking shape. A pre-assessment can confirm you’re on track before the formal process begins.

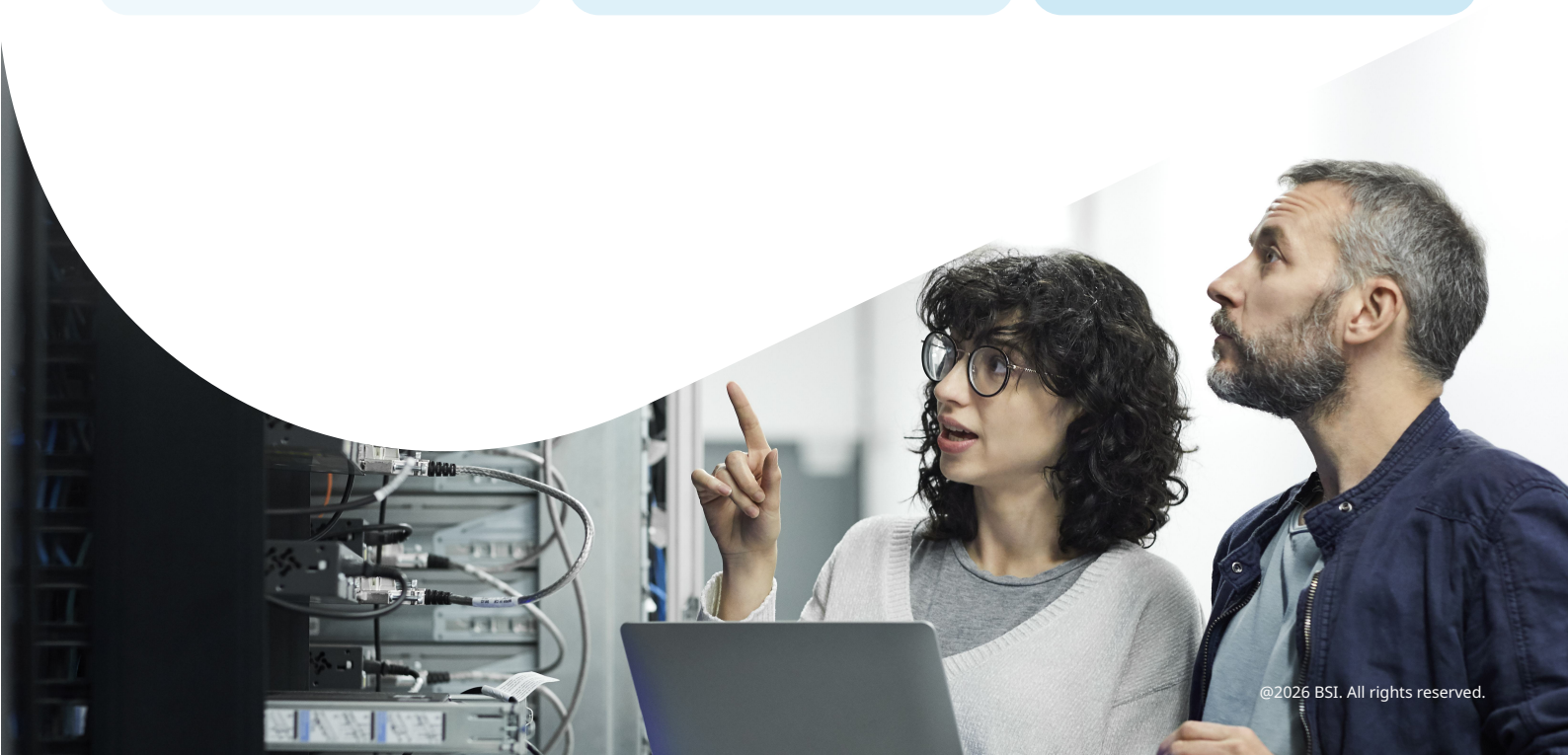
Learn more >

Mature stage

21-30 Points

Your controls look examination ready. The next step is starting the formal SOC 2 process, coordinated by BSI and performed by its partner CPA

Learn more >



Section 1 • Scope, Client Requirements & Risk Context

		Yes	No
1	Have you identified which of your clients or prospects require a SOC 2 report?	☐	☐
2	Do you understand that Security (Common Criteria) is mandatory for all SOC 2 examinations, and have you identified which additional criteria apply to your services (Availability, Processing Integrity, Confidentiality, Privacy)?	☐	☐
3	Have you mapped the systems and data that would be in scope for a SOC 2 examination?	☐	☐
4	Is SOC 2 readiness recognized as a business priority by leadership?	☐	☐

Section 2 • Security

5	Do you have documented access control policies (e.g. least privilege, role-based access)?	☐	☐
6	Are systems protected against unauthorized access (e.g. MFA, firewalls, intrusion detection)?	☐	☐
7	Are security incidents logged and reviewed regularly?	☐	☐
8	Are changes to systems and infrastructure formally authorized and tracked?	☐	☐

Reset checklist

Section 3 • Availability & Processing Integrity

		Yes	No
9	Do you have documented availability commitments to clients (e.g. SLAs)?	☐	☐
10	Are backup and disaster recovery procedures in place and tested?	☐	☐
11	Are processes in place to ensure data processing is complete, accurate and timely?	☐	☐
12	Is system capacity monitored to prevent performance-related disruptions?	☐	☐

Section 4 • Confidentiality & Privacy

13	Is confidential client data classified and handled according to defined policies?	☐	☐
14	Are data retention and disposal procedures documented and followed?	☐	☐
15	Do you have documented privacy commitments (notices/ policies) describing how personal data is collected, used, retained, disclosed, and disposed of?	☐	☐
16	Are data subject access or correction requests handled through a defined process?	☐	☐

Reset checklist

Section 5 • Governance & Risk Management

	Yes	No
17 Do you have a named owner accountable for information security and compliance?	☐	☐
18 Are risk assessments conducted on a regular basis?	☐	☐
19 Are policies reviewed and updated at least annually?	☐	☐
20 Is staff security awareness training conducted regularly?	☐	☐

Section 6 • Vendor & Third-Party Risk

21 Do you maintain an inventory of subcontractors/vendors with access to client data?	☐	☐
22 Are vendor security practices assessed before onboarding?	☐	☐
23 Are data protection and confidentiality clauses included in vendor contracts?	☐	☐
24 Is vendor performance and risk reviewed on an ongoing basis?	☐	☐

Reset checklist

Section 7 • Monitoring, Evidence & Examination Readiness

25	Do you maintain evidence of control operation (logs, approvals, records) on an ongoing basis?	☐	☐
26	Have you previously undergone any third-party certification or examination (e.g. ISO 27001 certification, SOC examination, or similar)?	☐	☐
27	Could you currently produce evidence of your controls operating over a 3-12-month period?	☐	☐
28	Do you have an internal process for tracking and remediating control gaps?	☐	☐
29	Is someone in your organization responsible for coordinating an external SOC examination engagement?	☐	☐
30	Are you prepared to undergo an independent SOC 2 readiness assessment?	☐	☐

Also offering: SOC 1 Attestation

If your organization provides services that affect your clients’ financial reporting such as payment processing, payroll, or claims management SOC 1 (SOC for Service Organizations: Internal Control over Financial Reporting, ICFR) may be more relevant than SOC 2. Speak to a BSI specialist to understand which report is right for your organization. **Contact Us**

Your SOC 2 readiness results

Your score 0/30	0 - 10 points =	Early Stage
	11- 20 points =	Developing Stage
	21-30 points =	Mature Stage

Reset checklist



If you scored 0–10 points

Early Stage: Start mapping your path to SOC 2

Every organization starts somewhere, and understanding where you stand today is genuinely valuable it means you can focus your energy on what matters most. At this stage, the most impactful work tends to be foundational: confirming which Trust Services Categories apply to you, understanding what your clients are asking for, and getting a clear picture of the systems and data in scope.

Many of the building blocks overlap with ISO/IEC 27001, so if your organization already holds that certification, you have a head start. From here, the next useful step is understanding the SOC 2 process itself — what's involved, what evidence is needed, and what a realistic timeline looks like for your organization.

[Learn more about SOC 2 attestation >](#)



If you scored 11-20 points

Developing Stage: Confirm you're on track with a pre-assessment

Having core controls in place is a real achievement it means your organization has already done the harder work of getting started. The natural next step is confirming those controls are operating consistently enough to stand up to independent examination, and identifying any gaps before the formal process begins.

BSI offers an optional pre-assessment ahead of formal SOC 2 attestation, designed to help you confirm any gaps in your implementation before proceeding — a useful way to walk into the formal assessment with confidence rather than surprises.

[Enquire about a SOC 2 Pre-Assessment](#)





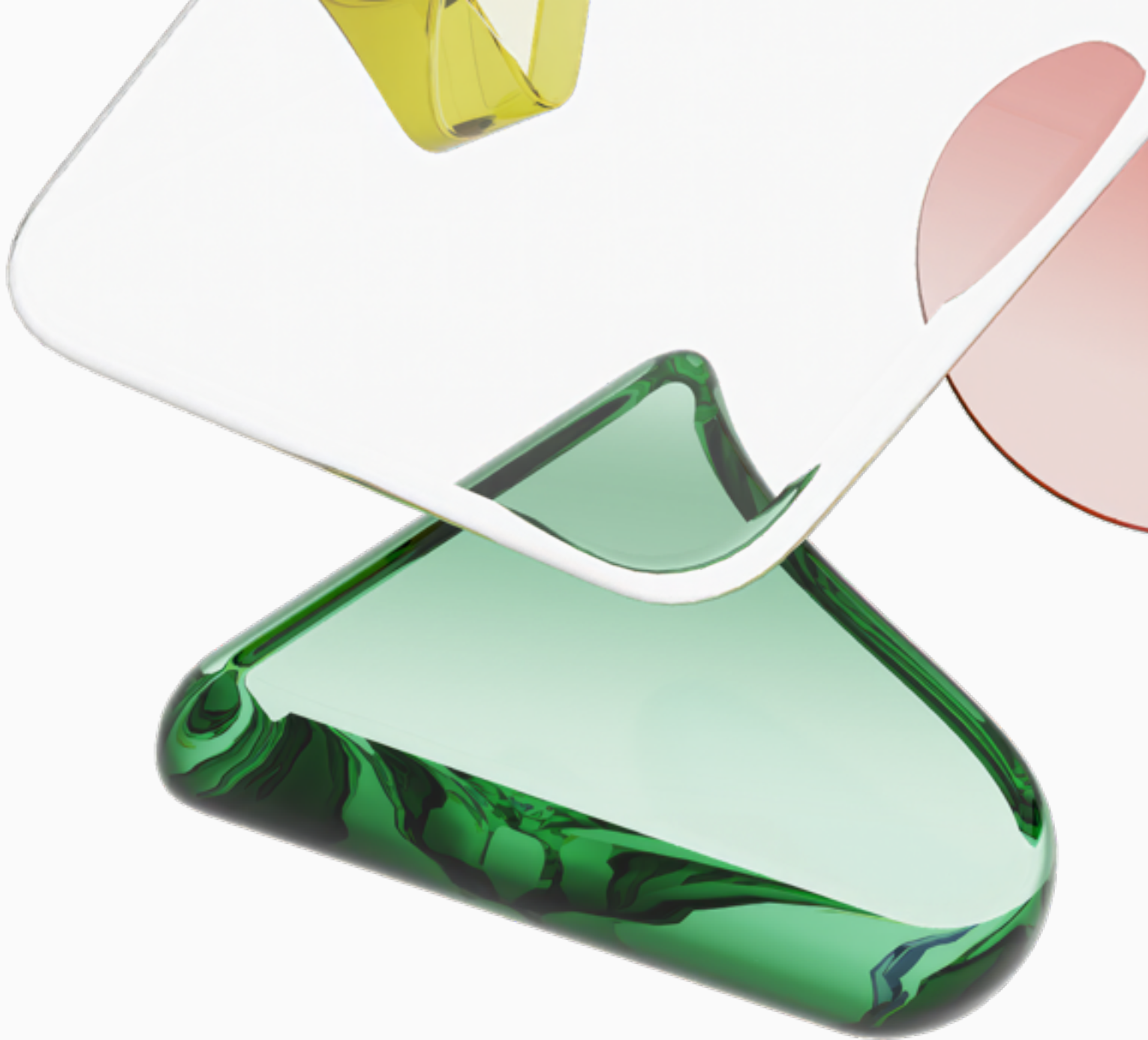
If you scored 21-30 points

Mature Stage: You're ready — start your SOC 2 attestation journey

A strong score here reflects consistent, well-managed practice the kind that doesn't happen by accident. Your organization has built a control environment that's ready for a formal SOC 2 examination, which means the question now shifts from 'are we ready?' to 'how do we get started?'

Partnering with BSI for SOC 2 attestation gives you a single point of contact and globally recognized expertise across ISO/IEC 27001 and related frameworks. BSI coordinates the whole process — application, kick-off, evidence collection and reporting while the examination and report signing are carried out by a licensed partner CPA firm.

[Talk to BSI about SOC 2 Attestation](#) >



Your partner
in progress