

Build trust and differentiate

with SOC 2 attestation

Navigating the Security and Privacy landscape

As digital ecosystems expand, the global security and privacy landscape is facing unprecedent pressure. Organizations worldwide are navigating a surge in cyber threats, evolving regulations, and rising expectations for trust and transparency.

©2025 BSI. All rights reserved.

$23 trillion

Cybercrime is projected to cost the world $23 trillion by 2027, a 175% increase from 2022 Source

63%

63% of data breaches are caused by third-party vendors Source

60%

60% of supply chain organizations will use cybersecurity risks as critical evaluation criteria for third-party business engagements and transactions Source

For organizations providing business-to-business services involving sensitive or personal data, there is an increasing need to back up a robust posture on cybersecurity, demonstrated through best practice processes and controls, with detailed evidence that the implemented controls are working effectively over time.

Key challenges when handling sensitive or personal data as a service Organization

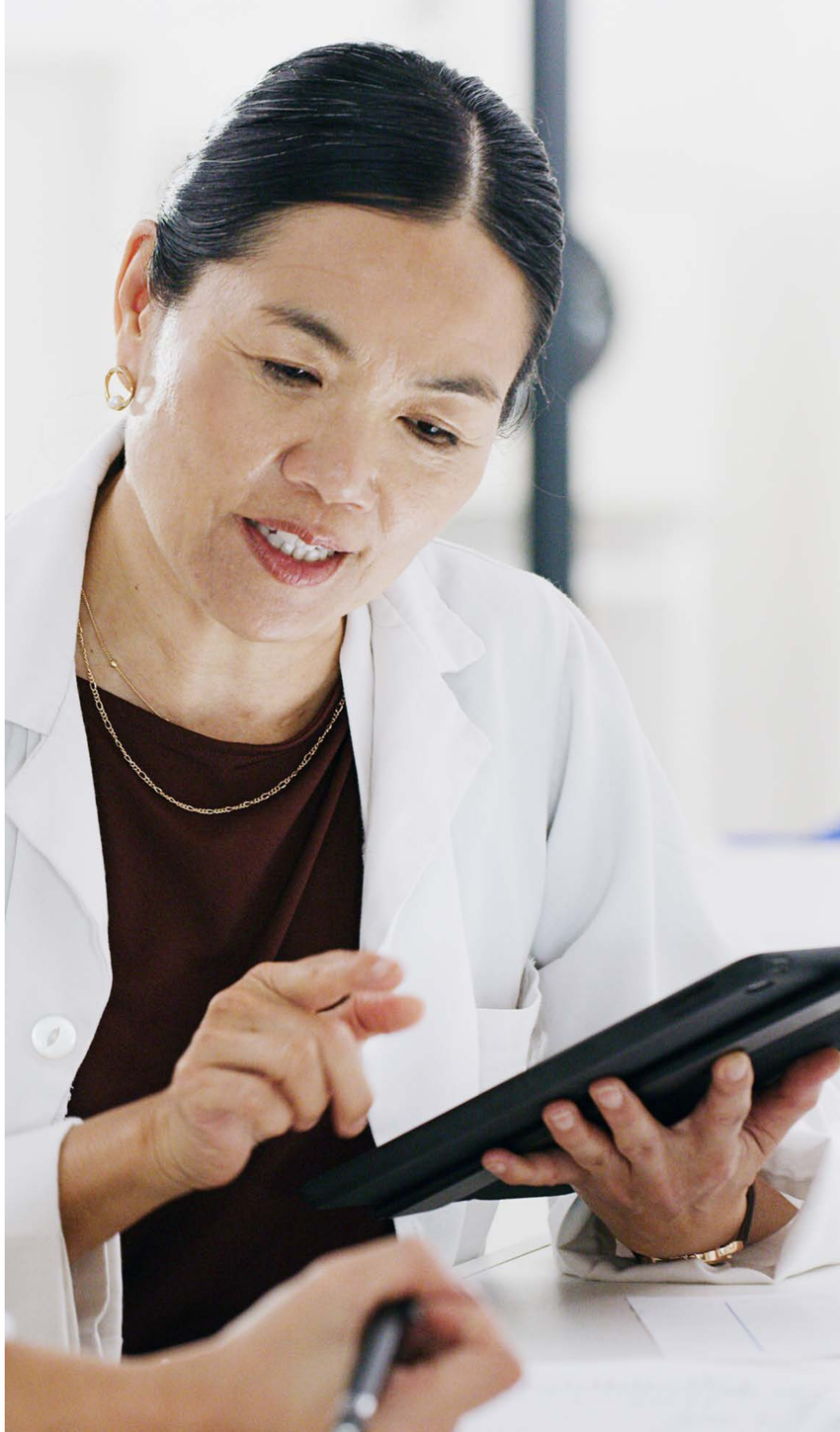
Security – the foundation of digital trust: how do you assure that the data is protected from unauthorized access, disclosure or damage?

Availability – an essential commitment for any service provider: how do you assure that the data and the associated service are available in accordance with Service Level Agreements, particularly in a landscape of “denial of service” and ransomware attacks?

Confidentiality – critical for sensitive data: how do you assure that data marked as confidential is suitably protected from unauthorized access?

Privacy – a fundamental human right and subject of extensive legislation globally. How do you assure that personal data is handled appropriately, through collection, use, retention, disclosure and disposal?

Processing Integrity – a vital component of a trusted service: how do you assure that data processing is complete, accurate, timely and authorized?



Position your organization as a trusted partner with SOC 2

SOC stands for System and Organization Controls, SOC 2 is a trusted security examination and report process created by the American Institute of Certified Public Accountants (AICPA,) that verifies how well an organization protects customer data. It's a mark of operational integrity, proving your systems are secure, available, and built to safeguard privacy. The report and associated attestation is provided by a Certified Public Accountant, and is performed in accordance with AICPA's standards.

SOC 2 is most valuable for:

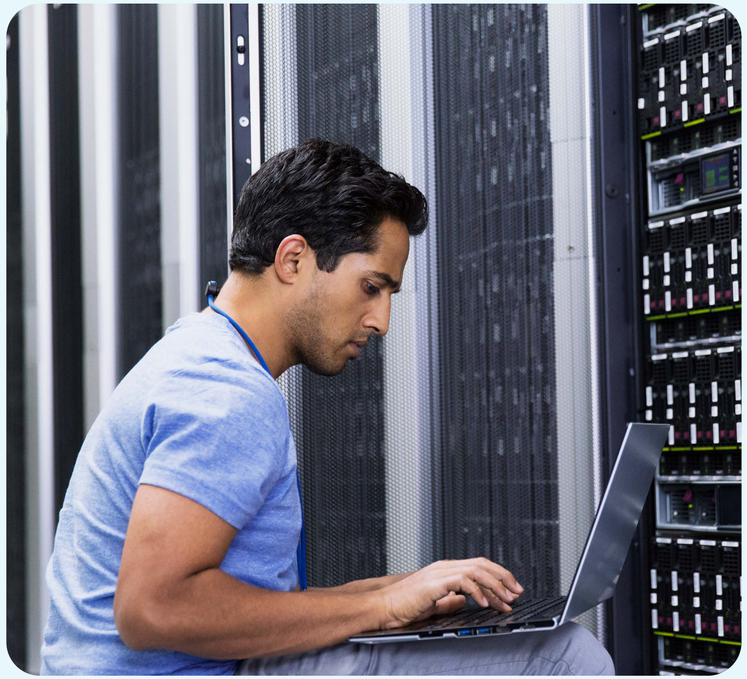
- US Based Companies
- Companies doing business with US customers
- International companies interested in entering or expanding in the US market

SOC 2 is particularly aimed at B2B service providers, especially those whose operations may impact their clients' financial reporting, offering targeted assurance that complements the broader, risk-based scope of ISO/IEC 27001. Get the best of the expertise in International Standard Management Systems certification and SOC services.

SOC 2 Attestation: A key differentiator

SOC 2 Attestation is an independent examination that demonstrates, through a report, how an organization manages and protects customer data based on defined trust principles.

It provides assurance to clients that robust controls are in place for security, availability, confidentiality, processing integrity and privacy.



Opportunities with SOC 2 attestation

Earn Client Confidence – Provides evidence to U.S. clients that your services meet key trust criteria like security and privacy.

Accelerate Sales Cycles – Speeds up due diligence by providing a verified, client-facing security report.

Strengthen Market Position – Differentiates you with independent assurance of how customer data is protected.

Enable U.S. Market Access – Meets expectations for service providers that may impact client financial reporting.

SOC 2 benefit

72% of organizations that achieved SOC 2 Type 2 compliance reported improved data security practices Source

The attestation journey

By gaining an SOC 2 report and attestation you can give clear evidence that your organization has implemented appropriate security controls for a digital services organization, and that the controls are working effectively.

With SOC 2, there are two types of report:

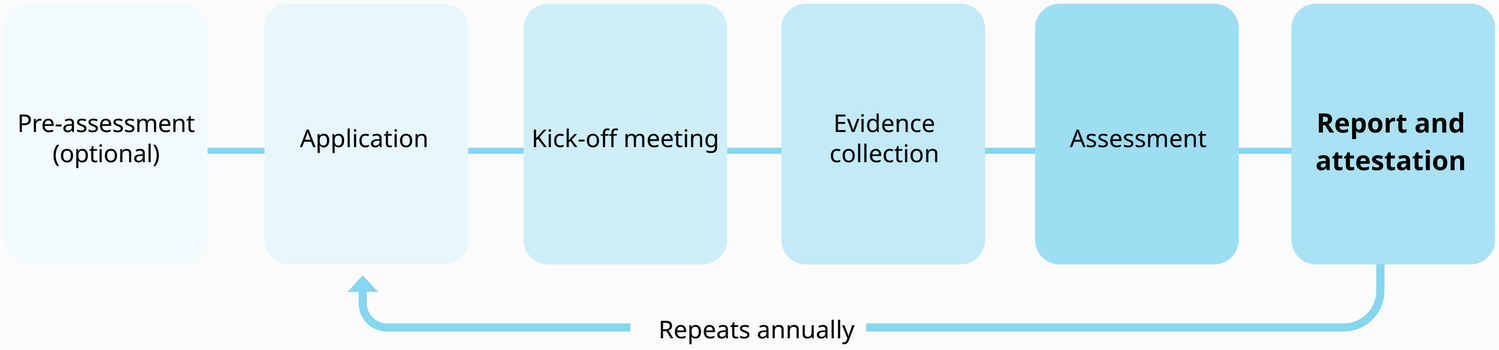
Type 1: An optional initial ‘moment in time’ report to check all the appropriate controls have been designed correctly.

Type 2: Assesses the operational effectiveness of the controls over time – typically requires 12 months of data.

Want to confirm you are ready to move forward with attestation? We offer an optional Pre-Assessment that can help you confirm any gaps in your implementation before proceeding with the formal assessment.



SOC 2 Process



Your partner in progress

Partnering with BSI for SOC 2 attestation means working with a globally recognized, independent assurance provider trusted by clients and regulators alike. Our deep industry expertise ensures your controls align with best practices and broader frameworks like ISO/IEC 27001. We can help you with assessing or integrating an assessment for SOC 2 and any other existing security frameworks.

We take a holistic approach—helping you embed resilience, improve security, and build stakeholder trust. With global reach and digital delivery, we support your growth wherever you operate. Our impartial assessments enhance your credibility and reduce compliance risk.

Make SOC 2 attestation your differentiator — gain credibility, trust, and competitive advantage with BSI as your partner.

Contact us today to learn more about the process and how to get started.

Learn more