



# **SERVICE-METHODE FÜR SOC-Zertifizierung**

**KONTROLLE DER SERVICE-ORGANISATION**

## Was sind SOC-Berichte?

**SOC-Berichte** sind eine Möglichkeit für Unternehmen, dies mithilfe unabhängiger Drittparteien zu überprüfen Dienstleister verfügen über entsprechende Kontrollen und halten sich an Branchenstandards Auslagerung einer Geschäftsfunktion an diese Organisation. Dies gibt Dienstleistern eine Chance Glaubwürdigkeit und Vertrauen bei Kunden, Investoren, Geschäftspartnern und Prüfern aufzubauen und sich gleichzeitig einen Wettbewerbsvorteil auf dem Markt verschaffen. Alle SOC-Untersuchungen werden durchgeführt gemäß

AICPA-Richtlinien:

Während des Prozesses von **SOC-Implementierung** ein erfahrenes Team von Technologieberatern und Prüfer arbeiten eng mit der Führung Ihrer Organisation zusammen, um sicherzustellen, dass:

- Der endgültige SOC-Bericht wird gründlich und zeitnah auf die individuellen Bedürfnisse einer Organisation zugeschnitten
- Geschäftsabläufe und interne Kontrollprozesse werden rationalisiert
- Vertragliche Verpflichtungen und Marktbedenken werden erfüllt
- Die AICPA-Berichtsanforderungen werden erfüllt

## Wie bestimme ich die Art des SOC-Berichts? Meine geschäftlichen Anforderungen?

Es gibt zwei Hauptgründe für eine SOC-Bewertung und -Zertifizierung:

- Ein Kunde, potenzieller Kunde oder Prüfer fordert einen SOC-Bericht an
- Ihre Organisation beschließt, proaktiv die Einhaltung der Sozialstandards zu gewährleisten

Im ersten Szenario könnte der Anforderer wahrscheinlich die Art des benötigten SOC-Berichts angeben. In beiden In diesem Szenario muss eine Organisation zunächst über ihre Ziele nachdenken. Normalerweise das gewünschte Ergebnis für jeden Eine Organisation muss ihr Engagement für ein angemessenes Design und einen effektiven Betrieb unter Beweis stellen seines internen Kontrollumfelds.

## Vergleichstabelle SOC 1, 2 und 3

Es gibt drei verschiedene Arten von SOC-Berichten: SOC 1, SOC 2 und SOC 3. Jeder Bericht unterscheidet sich jedoch liefert wertvolle Informationen, die zur Beurteilung der damit verbundenen Risiken und internen Kontrollen erforderlich sind mit einem externen Dienstleister. Für die Prüfung ist ein unabhängiger externer Prüfer erforderlich und bestätigen Sie verschiedene Aspekte einer Organisation, bevor Sie den Abschlussbericht erstellen.

<b>SOC 1</b>	<b>SOC 2</b>	<b>SOC 3</b>
<p>Berichten Sie über Ihre internen Kontrollen im Zusammenhang mit Finanzinformationen oder Aussagen</p> <p>Meistens an Prüfer weitergegeben</p> <p>Gilt für Unternehmen welche finanztechnisch abwickeln Informationen wie Medicals Schadensbearbeitung, Lohn- und Gehaltsabrechnung Dienstleistungen, Kreditunternehmen usw</p>	<p>Berichten Sie über Ihre internen Kontrollen im Zusammenhang mit fünf Vertrauensdiensten Prinzipien: Sicherheit, Verfügbarkeit, Integrität, Vertraulichkeit und Privatsphäre</p> <p>Meistens an Kunden weitergegeben und Stakeholder</p> <p>Gilt für jedes Technologieunternehmen Das ist die Informationsverarbeitung. Sowohl produkt- als auch servicebasiert Unternehmen</p>	<p>Bericht über die Ergebnisse von SOC 2 in geeigneter Weise an das öffentliche Publikum</p> <p>Für die breite Öffentlichkeit freigegeben</p> <p>Gilt für jede Öffentlichkeit Unternehmen, das eine SOC 2 verifiziert und gewünschtum einen SOC 3-Bericht zu erstellen für ein größeres Publikum</p>

## SOC 1-ZERTIFIZIERUNG

Ein SOC 2-Bericht konzentriert sich auf die Kontrollen Ihrer Organisation, die für die Finanzen einer Benutzerentität relevant sind. Es handelt sich um eine äußerst detaillierte Untersuchung, die ein spezielles Verständnis des Themas erfordert. Typischerweise gibt die Serviceorganisation dies vor und damit verbundene Kontrollaktivitäten basierend auf den von ihnen erbrachten spezifischen Dienstleistungen.

Ein SOC 1-Bericht umfasst im Allgemeinen Geschäftsprozesskontrollen, die den Betrieb betreffen. Ein SOC 1-Bericht umfasst im Allgemeinen Geschäftsprozesskontrollen im Hinblick auf die Vollständigkeit und Richtigkeit von Transaktionen sowie allgemeine Kontrollen der Informationstechnologie, wie z. B. Netzwerksicherheit und logischer Zugriff.

Aufgrund des begrenzten Umfangs eignet sich ein SOC 1-Bericht am besten für Organisationen, die Informationen vermitteln müssen. Dies ist erforderlich, wenn die Benutzereinheit börsennotiert ist und SOX 404 oder ähnliches einhalten muss. Hier einige Beispiele:



**Aufzeichnungen  
Dienstleistungen**



**Medizinische  
Ansprüche  
Verarbeitung**



**Lohn- und  
Gehaltsabrechnungsdienste**



**Kreditdienstleistungen**

## SOC 2-ZERTIFIZIERUNG

Ein SOC 2-Bericht ist für Serviceorganisationen gedacht, deren Benutzerentitäten nicht unbedingt antworten Kontrollen für die Finanzberichterstattung, die es Anbietern ermöglichen, die Anforderungen eines breiteren Spektrums von zu erfüllen Benutzerentitäten.

Eine SOC 2-Prüfung konzentriert sich in erster Linie auf die Art und Weise, wie Daten gespeichert und geschützt werden Kontrollen im Zusammenhang mit den Serviceverpflichtungen und Systemanforderungen basierend auf den AICPA's Kriterien für Vertrauensdienste (unten definiert).

- **Sicherheit**- Informationen und Systeme sind vor unbefugtem Zugriff und Offenlegung geschützt von Informationen
- **Verfügbarkeit** - Informationen und Systeme stehen für den Betrieb und die Nutzung zur Erfüllung der Anforderungen des Unternehmens zur Verfügung Ziele
- **Verarbeitungsintegrität** - Die Systemverarbeitung ist vollständig, gültig, genau, zeitnah und befugt, die Ziele des Unternehmens zu erreichen
- **Vertraulichkeit** - Als vertraulich gekennzeichnete Informationen werden geschützt, um den Anforderungen des Unternehmens gerecht zu werden Ziele
- **Privatsphäre** - Persönliche Daten werden gesammelt, verwendet, gespeichert, offengelegt und zur Erfüllung der Anforderungen entsorgt die Ziele des Unternehmens

SOC 2-Berichte können von jedem Technologieunternehmen genutzt werden, das sich mit Informationen beschäftigt Verarbeitung. Während SOC 1- und SOC 2-Berichte beide eine eingeschränkte Zielgruppe haben, sind SOC 2-Berichte eingeschränkt können an andere Parteien wie potenzielle Kunden oder das Lieferantenmanagement weitergegeben werden Fachleute, Aufsichtsbehörden und andere wichtige Geschäftspartner.

## SOC 3 CERTIFICATION



Wie SOC 2 konzentrieren sich auch SOC 3-Berichte auf Kontrollen, die für die fünf Vertrauensdienste der AICPA relevant sind Kategorien. Im Gegensatz zu SOC 2 sind SOC 3-Berichte jedoch zertifiziert und können öffentlich gemacht werden verfügbar, was sie zu wertvollen Instrumenten für die Vermarktung der Wirksamkeit Ihrer Kontrolle macht Umfeld.

Wenn Sie einen SOC 3-Bericht wünschen, muss Ihre Organisation zunächst einen SOC 2, Typ 2 ausfüllen Untersuchung (mehr zu Berichtstypen weiter unten). Es können SOC 2- und SOC 3-Prüfungen durchgeführt werden auf einer oder mehreren der Vertrauensdienstkategorien. SOC 3-Berichte enthalten weitgehend das Gleiche Informationen, die in SOC 2-Berichten enthalten sind, außer mit einer weitaus weniger detaillierten Beschreibung Ihrer Person Kontrollen im Zusammenhang mit Compliance und Betrieb. Sie beinhalten auch keine spezifische Kontrolle Aktivitäten, Testverfahren oder detaillierte Ergebnisse zur betrieblichen Wirksamkeit.

## TYP 1 vs. TYP 2

Alle SOC-Berichte (außer SOC 3) können entweder Typ 1 oder Typ 2 sein. Der Unterschied ist hauptsächlich basierend auf dem Zeitraum im Geltungsbereich

- **Bericht vom Typ 1** : Ein TYP-1-BERICHT beschreibt die Eignung einer Serviceorganisation Entwurf und Implementierung von Kontrollen zu einem bestimmten Zeitpunkt
- **Bericht vom Typ 2** : Ein TYP-2-BERICHT stellt sicher, dass definierte Kontrollaktivitäten konsistent sind effektiv über einen definierten Zeitraum arbeiten, der normalerweise zwischen 6 Monaten und 1 Jahr liegt, Dies führt zu einer verbesserten Betriebsleistung

In vielen Fällen beginnt eine Serviceorganisation mit einem Bericht vom Typ 1, um die Kontrolle zu definieren Aktivitäten zu einem bestimmten Zeitpunkt. Sobald die Kontrollen entworfen und implementiert sind, wird der Typ 2 verwendet Bericht würde folgen. Da der Typ-2-Bericht einen Zeitraum abdeckt (d. h. 6 oder 12 Monate), ist dieser Bericht wertvoller für Benutzer, da es sicherstellt, dass die Kontrollen während eines bestimmten Zeitraums in Betrieb waren effektiv. Eine Organisation beauftragt in der Regel eine Wirtschaftsprüfungsgesellschaft mit der Erstellung des Typ-2-Berichts. jährlich.

## Wie bereite ich mich auf eine SOC-Bewertung vor?

Wenn Sie mit Ihrer ersten SOC-Bewertung beginnen, ist es von Vorteil, mit dem von Ihnen ausgewählten Drittanbieter zusammenzuarbeiten. Beauftragen Sie einen Berater wie uns damit, eine erste Lückenbewertung durchzuführen, damit Sie etwaige Lücken schließen können vor Beginn des SOC-Berichtsprozesses. Dieser Weg hilft Ihnen, das Vorhandene zu füllen. Sie schließen Lücken in Ihrem aktuellen System und sorgen so für ein viel konformeres System, das sehr nah beieinander ist zur Erfüllung der SOC-Anforderungen. Obwohl jeder SOC-Bericht einen unterschiedlichen Umfang hat, gibt es bestimmte Schwerpunkte, die für alle SOC-Bewertungen von wesentlicher Bedeutung sind. Durch die Konzentration auf die folgenden Aufgaben kann eine Organisation damit beginnen, ihre Mitarbeiter auf ein stärkeres Kontrollumfeld vorzubereiten, daher eine effizientere SOC-Bewertung.

### DOKUMENTATION

Aus der Sicht eines Prüfers gilt: Wenn etwas nicht dokumentiert ist, existiert es nicht. Obwohl es möglich ist, wenn strenge interne Kontrollen vorhanden sind, werden die Beweise für das Vorkommen möglicherweise nicht in Erinnerung gerufen. Sicherstellen, dass die Dokumentation gepflegt wird, um alle vorhandenen Kontrollen zu unterstützen (z. B. Genehmigung für Zugangsgewährung, Mitarbeiteranerkennungen, Pflege von Bevölkerungsgruppen usw.).

### DEFINIERTER RICHTLINIEN UND VERFAHREN

Um sicherzustellen, dass alle relevanten Parteien ihre Verantwortung zur Erfüllung organisatorischer Anforderungen verstehen, stellen Sie sicher, dass grundlegende Prozesse und Verfahren dokumentiert werden. Dies bietet eine Ressource für Mitarbeiter und Prüfer, um die Absichten der Organisation zu verstehen und die Kontrollumgebung. Der Umfang der Richtlinien sollte Folgendes umfassen:

- » Organisatorische Abläufe zur Erfüllung vertraglicher Verpflichtungen
- » Mittel zur Erfüllung grundlegender Serviceverpflichtungen und Systemanforderungen
- » Risikomanagementansatz

### RISIKOBEWERTUNG

Ein formalisierter Prozess, der durch eine jährliche Risikobewertungsdiskussion erleichtert und von der genehmigt wird. Es sollte ein Vorstand bzw. eine Geschäftsleitung vorhanden sein. Anstelle eines formellen jährlichen Risikos aufgrund der Bewertung kann sich eine Organisation auch dazu entschließen, vierteljährliche Treffen abzuhalten, um Änderungen zu besprechen, Bedrohungen, Geschäftsabläufe usw. und deren Auswirkungen auf die Gesamtrisikobewertung. Das Risiko der Bewertung sollte definierte Risikostufen (d. h. niedrige, mittlere und hohe Bedrohung) umfassen. Der Abhilfeansatz des Unternehmens (d. h. akzeptieren, abschwächen oder beseitigen) mit Einzelheiten dazu, wie das Problem behoben wird. Das Unternehmen hat reagiert oder plant, in Zukunft zu reagieren.

# SOC-Implementierungs-Roadmap

Obwohl jeder SOC-Bericht unterschiedliche Anforderungen und Ziele hat, wird jeder im Allgemeinen durchgeführt folgenden sieben Hauptphasen

PROZESSPHASE	WICHTIGSTE TEILNEHMER	SCHLÜSSELMATERIALIEN
1 Scoping	Top-Management Wirtschaftsprüfer, Berater	Hintergrundinformationen zur Organisation Bedürfnisse und Kundenanforderungen
2 Komplettlösung und Kontrolldesign	Berater, Prozessverantwortliche	Bestehende Richtlinien und Verfahren, Materialien aus der Zeit, die mit jedem Prozessverantwortlichen verbracht wird
3 Lückenbewertung	Berater, Prozessverantwortliche	Vorläufige Dokumentation zu Unterstützung der Sanierungs-Roadmap
4 Sanierung	Berater, Prozessverantwortliche	Dokumentation zur Validierung der Kontrollumgebung
5 Prüfungstests	Auditor, Berater, Prozess Eigentümer	Prozessdokumentation, Prüfungsnachweise
6 Bericht	CPA-Prüfer	Richtlinien und Verfahren, Entwurfsfeedback, Reaktion auf Rückmeldungen und Ausnahmen
7 Ausgabe	CPA-Prüfer	SOC-Bericht

Auch bei Prüfungen im ersten Studienjahr können die meisten Prüfungsabschnitte innerhalb einer definierten Frist absolviert werden. Der Zeitplan ist zwar die unvorhersehbarste Phase, aber die Sanierung (Stufe 4). Der Sanierungsaufwand wird anhand der Ergebnisse der Lücke ermittelt. Beurteilung (Stufe 3). Während der Bewertungsphase wird Ihr Wirtschaftsprüfungsunternehmen eine Abhilfe schaffen Roadmap, um die Einhaltung der geltenden SOC-Kriterien sicherzustellen. Durch die Schaffung einer starken Kontrolle Umgebung vor Beginn der Prüfung legen Sie den Grundstein für eine organisierte, minimal störende Prüfung.

## SOC Audit Services

Unser erfahrenes Team berät Serviceorganisationen zu den AICPA-SOC-Berichtsanforderungen. Wir liefern wertvolle Informationen, die Kunden, Interessenten und Prüfer zur Beurteilung benötigen die Risiken und internen Kontrollen, die mit einem ausgelagerten Dienstleister verbunden sind.

Als qualifiziertes Beratungsunternehmen in diesem Bereich haben wir unzählige Gespräche geführt Bildung, Wert und Effizienz. Wir sind stolz darauf, mit Organisationen zusammenzuarbeiten, die spezifische Anforderungen erfüllen Bedürfnisse, konkurrierende Prioritäten, Zeitbeschränkungen und andere einzigartige Ziele. Wir verstehen das Wert auf Zeit, angemessene Planung und Ausbildung, die einen reibungslosen Ablauf der Prüfung gewährleisten schreitet voran.

## Über TOPCertifier

TOPCertifier ist eine weltweit anerkannte Unternehmensberatung mit Spezialisierung auf Informationen Sicherheitsdienste und soziale Beurteilungen.

Wir haben unseren Hauptsitz in Bangalore (Indien) und sind mit einem Spezialgebiet in über 20 Ländern tätig Der Fokus liegt auf den USA, Europa und den Golfstaaten. Auch in Asien verfügen wir über eine beeindruckende Präsenz-Pazifische und afrikanische Regionen. Wir haben über 2.800 Organisationen beraten, darunter zahlreiche Branchen, in den Bereichen Buchhaltung, Steuern, Rentabilität und Geschäftsprozesslösungen, seit unserer Gründung im Januar 2010. Mit einem Team von über 200 branchenerfahrenen Beratern, zertifizierten leitenden Auditoren und Als Fachexperten haben wir in Bezug auf unsere Zertifizierung eine 100-prozentige Erfolgsbilanz vorzuweisen Erfolgsquote.



**Danke**

**Um mehr zu erfahren,  
BESUCHEN [WWW.TOPCERTIFIER.COM](http://WWW.TOPCERTIFIER.COM)**