Infosheet

Mehr Wert.
Mehr Vertrauen.

System- und Organisations-kontrollen: Ihr SOC 2-Nachweis (Typ 1 & 2)

Ihre Herausforderung
Der konsequente Schutz von Kundendaten ist heutzutage das Fundament für Geschäftsfähigkeit. Dienstleister müssen sicherstellen, dass die erforderlichen Kontrollen und Verfahren vorhanden sind, um das Risiko einer Sicherheitsverletzung zu minimieren und die Vertraulichkeit der Kundendaten zu gewährleisten.
Speziell für Unternehmen, die auf dem US-Markt aktiv sind, hat sich dafür SOC 2 etabliert. Ein entsprechender Nachweis belegt, dass ein Unternehmen einen umfassenden Ansatz für Datensicherheit verfolgt. SOC-Konformität wird zunehmend zu einer Mindestanforderung für Dienstleister.

Was ist SOC 2 konkret?
Der SOC 2-Standard für Informationssicherheit wurde vom American Institute of Certified Public Accountants (AICPA) entwickelt – von Wirtschaftsprüfern für Wirtschaftsprüfer. SOC steht für Systems and Organizations Controls (System- und Organisationskontrollen) und ist insbesondere in den USA etabliert. Der Prüfstandard richtet sich an Unternehmen mit einem Portfolio aus IT und Datenschutz, beispielsweise an SaaS-Anbieter, Tech-Firmen und andere Dienstleister, die Kundendaten verarbeiten. Er hilft ihnen dabei, Compliance-Anforderungen zu erfüllen, Vertrauen zu schaffen, interne Prozesse zu verbessern und Wettbewerbsvorteile zu erzielen.

Die Basis des Standards sind fünf Vertrauensprinzipien, die Trust Services Criteria (TSC): Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz. Beim SOC 2-Assessment legen Anwenderunternehmen selbst fest, welche TSC geprüft und bewertet werden sollen. Das AICPA definiert hierfür die allgemeinen und spezifischen Prüfkriterien.

Es gibt zwei Arten von SOC 2-Prüfungen:

- SOC 2, Typ 1: Bewertung der Angemessenheit und Ausgestaltung der Kontrollen zu einem bestimmten Zeitpunkt

- SOC 2, Typ 2: Bewertung der Wirksamkeit der implementierten Kontrollen über einen Zeitraum hinweg

Ein SOC 2, Typ-1-Audit lässt sich meist in wenigen Wochen bis zu zwei Monaten abschließen. Ein SOC 2, Typ-2-Audit umfasst einen Beobachtungszeitraum von gängigerweise 6 bis 12 Monaten. Der beglaubigte SOC 2-Prüfbericht ist anschließend 12 Monate gültig.

Keine Zertifizierung
Oftmals wird fälschlicherweise von einer SOC 2-Zertifizierung und einem SOC 2-Zertifikat gesprochen. Beides gibt es nicht. Nach SOC 2 geprüfte Unternehmen erhalten von TÜV SÜD einen Bestätigungsbericht, der von einem Wirtschaftsprüfer (CPA) mit einer Lizenz der AICPA beglaubigt wurde.

Was sind SOC 1 und SOC 3?
Neben SOC 2 gibt es auch SOC 1 und SOC 3. Der Hauptunterschied liegt in Zielgruppe und Prüfungsfokus. SOC 1 richtet sich an Unternehmen, die Finanztransaktionen für ihre Kunden abwickeln, und konzentriert sich auf interne Kontrollen mit Bezug zur Finanzberichterstattung. SOC 3 ist die öffentliche, komprimierte Variante des SOC 2-Berichts und besonders für Marketing und Kommunikation geeignet. SOC 3 bietet einen Überblick über Sicherheits- und Compliance-Maßnahmen, ohne dabei sensible Details offenzulegen.

Warum SOC 2 für Ihr Unternehmen wichtig ist
Heutzutage sorgen sich Kunden, Behörden und Geschäftspartner zunehmend darum, ob ihre Daten von den Dienstleistungsorganisationen angemessen geschützt werden. Dienstleister wiederum stehen vor der Herausforderung, ihren Kunden Datensicherheit anhand zahlreicher Standards und Frameworks nachzuweisen. SOC 2 schafft als etablierter, anerkannter Prüfstandard Abhilfe, reduziert Risiken, sorgt für Compliance und bringt Dienstleistern klare Wettbewerbsvorteile.

Wie TÜV SÜD Sie unterstützt
Wenn Sie sich für SOC 2 entschieden haben, kommen Sie zeitnah auf uns zu. Wir planen mit Ihnen die Audit-Durchführung, und unsere erfahrenen Auditoren mit höchstem Branchen-Knowhow begleiten Sie durch den gesamten SOC 2-Assessment-Prozess. Mit einem SOC 2-Prüfbericht von TÜV SÜD signalisieren Sie Ihren Kunden und Stakeholdern, dass Sie den Schutz ihrer sensiblen Daten ernst nehmen.

So profitiert Ihr Unternehmen von einem SOC 2-Nachweis
- Wettbewerbsvorteile: Geben Sie Ihren Stakeholdern und Kunden die Gewissheit, dass Sie höchste Standards der Informationssicherheit einhalten.
- Vertrauen: Überzeugen Sie Stakeholder mit Transparenz und erfüllen Sie vertragliche Anforderungen.
- Risikominimierung: Befassen Sie sich proaktiv mit Risiken, senken Sie Compliance-Kosten und verbessern Sie den Reifegrad der Kontrollen in Ihrem Unternehmen.

Warum TÜV SÜD?
Da TÜV SÜD herstellerunabhängig ist, sind unsere Audits durch Dritte unparteiisch und unabhängig. Unser globales Netzwerk erfahrener und hochqualifizierter Auditoren kann Sie mit Zertifizierungsdienstleistungen weltweit unterstützen. Mit einem ganzheitlichen Ansatz bieten unsere Experten IT-Zertifizierungen nach einer Vielzahl von internationalen Standards an. Mit unserem Zertifizierungszeichen zeigen Sie auf effiziente Weise Ihr Engagement für Compliance und Qualität.

Mehr Wert. Mehr Vertrauen.
TÜV SÜD ist ein zuverlässiger Partner der Wahl für Lösungen in den Bereichen Sicherheit und Nachhaltigkeit. Das Unternehmen ist auf die Prüfung, Zertifizierung und Auditierung von Dienstleistungen spezialisiert. Seit 1866 ist das Unternehmen seinem Ziel verpflichtet, Fortschritt zu ermöglichen, indem es Menschen, die Umwelt und Vermögenswerte vor technologiebedingten Risiken schützt. Mit mehr als 28.000 Mitarbeitern an über 1.000 Standorten schafft das Unternehmen einen Mehrwert für Kunden und Partner, indem es den Marktzugang ermöglicht und Risiken managt. Indem TÜV SÜD technologische Entwicklungen vorwegnimmt und den Wandel erleichtert, schafft das Unternehmen Vertrauen in eine physische und digitale Welt, um eine sicherere und nachhaltigere Zukunft zu schaffen.

TÜV SÜD Management Service GmbH Ridlerstraße 57, 80339 München, Deutschland
Tel.: 0800 5791-5000, ms-anfragen@tuvsud.com, tuvsud.com