SECURANCE

Stap-voor-stap Gids -

SOC 2 Compliance.

SOC 2 Compliance

Uitbesteding | Trust Services Criteria

SOC 2 is een Service Organization Control (SOC) rapport dat zekerheid biedt over uitbestede processen. Een audit uitgevoerd in overeenstemming met SOC 2 wordt algemeen erkend, omdat het een diepgaande audit van de controleactiviteiten van een serviceorganisatie vertegenwoordigt, waaronder controles op interne controle, beveiliging, risicomanagement en gerelateerde processen. SOC 2-rapporten worden opgesteld in overeenstemming met de Trust Services Criteria.

SOC 2 richt zich op de niet-financiële rapportagecontroles van een bedrijf met betrekking tot beveiliging, beschikbaarheid, verwerkingsintegriteit, vertrouwelijkheid en privacy. Deze principes zijn vastgelegd in de Trust Services Criteria. Elk van de criteria heeft gedefinieerde vereisten (Points of Focus) die als richtlijn dienen om de naleving van de criteria aan te tonen.

Modulair

SOC 2-rapporten zijn modulair, wat betekent dat rapporten een of meer van de principes kunnen dekken, afhankelijk van de behoeften en vereisten van een serviceorganisatie. De enige criteria die verplicht zijn voor SOC 2 zijn de beveiligingscriteria. Deze criteria worden ook wel de gemeenschappelijke criteria genoemd.

Common Criteria

De enige criteria die verplicht zijn voor SOC 2 is beveiliging, waarnaar ook wordt verwezen als de Common Criteria, Aanvullende criteria kunnen worden opgenomen binnen de reikwijdte van een SOC 2-rapportage.

Naast de beveiligingseisen (logische en fysieke toegangscontrole, systeembeheer en wijzigingsbeheer) bevatten de gemeenschappelijke criteria ook eisen voor een raamwerk voor interne controle, waaronder risicobeheer (COSO). De belangrijkste elementen van het COSO-raamwerk zijn Controleomgeving, Communicatie en Informatie, Risicobeoordeling en Risicobeperking, Bewakingsactiviteiten en Controleactiviteiten.

De gekozen criteria worden geïmplementeerd binnen de organisatie en uiteengezet in het SOC 2-rapport door het volgen van de aandachtspunten en aanvullende criteria zoals uiteengezet in het COSO-raamwerk 2013 (risicomanagement) en de Trust Services Criteria. Hierna wordt het SOC 2-rapport gecontroleerd door onafhankelijke accountantskantoren.

Trust Services Criteria

Criteria Uitgelegd

De enige verplichte criteria zijn de Beveiligingscriteria, zoals eerder beschreven. Vaker wordt de toepasbaarheid van de criteria Beschikbaarheid, Vertrouwelijkheid, Verwerkingsintegriteit en Privacy overwogen op basis van de geleverde diensten en in samenwerking met belangrijke klanten en SOC 2-experts. Wanneer een organisatie ervoor kiest om criteria op te nemen, moeten alle bijbehorende vereisten en aandachtspunten worden overwogen en geïmplementeerd indien van toepassing. De belangrijkste kenmerken per criterium worden hieronder beschreven.

SECURITY

Security refers to the protection of data throughout its life cycle. Security controls are put in place to protect against unauthorised disclosure, unauthorised access or damage to systems that could affect other criteria.

AVAILABILITY

Availability refers to controls that demonstrate that systems remain operational and perform to meet established business objectives and service level agreements.

CONFIDENTIALITY

Confidentiality requires companies to demonstrate their ability to safeguard confidential information throughout its lifecycle, including its collection, processing and disposal.

PROCESSING INTEGRITY

Integrity of use must ensure that data is processed in a predictable manner, without unexplained or random errors.

PRIVACY

Privacy is similar to Confidentiality, but has distinctive application to personally identifiable information (PII), especially information your organisation obtains from its customers.

FASE 1. SCOPEBEPALING

Hoe bepaal je de scope van een SOC 2-rapport

De scope van een SOC 2-rapport heeft betrekking op de (niet-financiële) controles binnen een serviceorganisatie die relevant zijn voor Beveiliging, Beschikbaarheid, Verwerkingsintegriteit, Vertrouwelijkheid en/of Privacy, zoals gedefinieerd in de Trust Service Criteria. Het SOC 2-rapport moet een sectie bevatten die de belangrijkste componenten van de scope vermeldt. Dit omvat details over het type dienst(en) dat wordt geleverd, evenals de infrastructuur, software, mensen, beleidsmaatregelen en procedures, en gegevens die relevant zijn voor die diensten.

Voorbeeld

Voor een Software-as-a-Service (SaaS)-provider omvat de scope doorgaans hun softwareapplicatie(s) die toegankelijk zijn voor hun klanten. Dit omvat alle gegevens die erin worden opgeslagen, de infrastructuur die de applicatie host, en de mensen en procedures die deze ondersteunen. Subserviceproviders en aanvullende controlegebieden voor gebruikersentiteiten geven verdere details over de scope in andere secties van het rapport door de grenzen van de scope binnen het rapport te definiëren.

Conclusie

Uiteindelijk ligt het bepalen van de scope van een SOC 2-rapport bij het management. De controles die betrekking hebben op de operaties van de serviceorganisatie en die essentieel zijn voor de niet-financiële verslaglegging van de organisatie, moeten binnen de scope vallen. Hoewel de scope duidelijk moet worden gedefinieerd en vermeld in het rapport, is er enige flexibiliteit. Uiteindelijk ligt de verantwoordelijkheid voor het waarborgen dat het rapport voldoet aan de vereisten van de eindgebruikers bij het management.

Concurrentievoordeel

Hoe een SOC 2-rapport je een voorsprong geeft op de concurrentie

SOC 2 biedt een concurrentievoordeel door serviceorganisaties te onderscheiden van hun concurrenten. De voordelen van SOC 2-rapporten omvatten het verbeteren en verfijnen van risicobeheer, terwijl ze tegelijkertijd het marktvertrouwen versterken door een transparante presentatie van het controleframework. De implementatie van SOC 2 verbetert de efficiëntie van audits en minimaliseert operationele inefficiënties binnen de organisatie.

FASE 2. Implementatie

Stap-voor-stap Aanpak

1. Impact Analyse & Planning

In Fase 1 wordt de impact (GAP-analyse) van de implementatie bepaald en wordt de toepasbaarheid van de Trust Services Criteria beoordeeld. Op basis van de impact en de vastgestelde scope van de implementatie wordt een gedetailleerd plan opgesteld, waarin de verschillende mijlpalen worden geïdentificeerd en afspraken met het management worden gemaakt.

2. Processen & Controls

In Fase 2 worden interviews gehouden om risico's te identificeren, de impact en de bestaande werkwijze te bepalen en kennis te nemen van de beschikbare informatie binnen de organisatie. Vervolgens worden de organisatorische beheersmaatregelen beschreven volgens de SOC 2-vereisten, op basis van de informatie verkregen uit de interviews. Deze worden vastgelegd in een controlematrix; een matrix waarin de SOC 2-vereisten en bijbehorende beheersmaatregelen worden opgenomen. We zullen proactief adviseren over de implementatie van ontbrekende controles (inclusief procesbeschrijvingen).

3. Control Framework

In Fase 3 beschrijft Securance het controle framework op basis van het meest recente COSO-framework (COSO 2013) en stelt het de algemene sectie van het rapport op. In deze algemene sectie wordt een beschrijving opgenomen van de processen, de organisatie en de algemene IT-controles.

4. SOC 2 Rapport

In Fase 4 wordt het volledige SOC 2-rapport opgesteld op basis van de afzonderlijke secties en aanvullende onderdelen, zoals de managementverklaring en de aanvullende gebruikerscontroles. Fase 4 resulteert in een conceptversie van het SOC 2-rapport. We zullen dit rapport in detail bespreken met relevante medewerkers. Tijdens deze fase zal de organisatie eventuele geïdentificeerde ontbrekende controles implementeren.

De doorlooptijd van de eerste vier fasen bedraagt tussen de zes en acht weken, afhankelijk van de inzet en beschikbaarheid van medewerkers. Van C-level executives wordt verwacht dat zij gedurende deze periode één dag per week beschikbaar zijn.

5. Pre-Audit

Na de voorbereiding van het rapport voert Securance in Fase 5 een pre-audit of 'walkthrough' uit. Tijdens de pre-audit worden de beheersmaatregelen getest en mogelijke probleemgebieden geïdentificeerd voorafgaand aan de definitieve audit. In deze fase verstrekt de organisatie de documentatie en bewijsmaterialen die Securance nodig heeft.

6. Rechtzetten

Tijdens Fase 6 worden, naar aanleiding van de pre-audit, verbeteringen in de beheersmaatregelen en het managementsysteem doorgevoerd en worden oplossingen voorbereid voor de vastgestelde probleemgebieden. Securance biedt oplossingen die binnen de organisatie en het SOC 2-rapport kunnen worden geïmplementeerd. Fase 6 resulteert in het definitieve SOC 2-rapport.

De doorlooptijd van Fase 5 en 6 bedraagt tussen de twee en vier weken. De verwachte beschikbaarheid van medewerkers is gedurende deze periode één dag per week.

FASE 3. De Audit

Quality Assurance Audits

The SOC 2 Audits Uitgelegd

De sleutel tot succesvol uitbesteden is het selecteren van een serviceprovider die uw organisatie begrijpt. Een SOC 2-certificering biedt zekerheid over de Beveiliging, Beschikbaarheid, Vertrouwelijkheid, Verwerkingsintegriteit en Privacy van informatie. Wanneer u werkt met gevoelige klantgegevens, zijn deze elementen cruciale succesfactoren.
In een SOC 2-rapport wordt het risicobeheersingskader beschreven, inclusief de bijbehorende controles en procedures voor het bewaken van dit kader. Het rapport wordt opgesteld volgens de **Trust Services Criteria**, die een set criteria bieden voor Beveiliging, Beschikbaarheid, Verwerkingsintegriteit en Privacy. Dit helpt organisaties om bij te blijven met de snelle groei van cloud computing en de uitdagingen van zakelijke outsourcing in de wereldwijde economie.

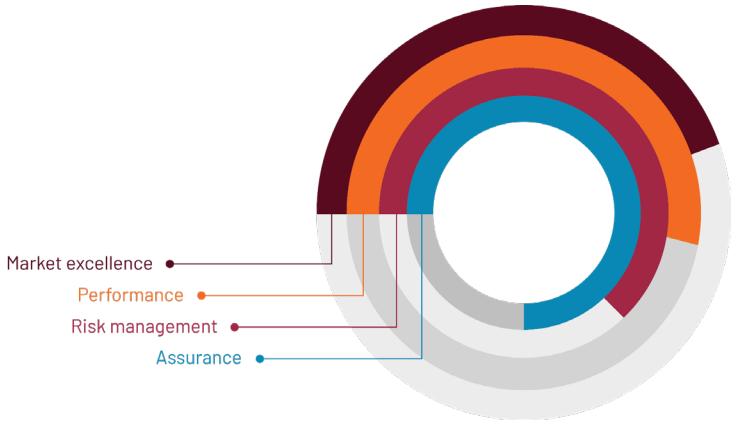
Type I Rapport

Een SOC 2 Type I-rapport bevat een oordeel van een externe auditor over de beheersmaatregelen die op een specifiek moment operationeel zijn. De externe auditor beoordeelt of de beheersmaatregelen adequaat zijn ontworpen om redelijke zekerheid te bieden dat de financiële verslaglegging correct is en of de controles daadwerkelijk zijn geïmplementeerd.

Type II Rapport

In een SOC 2 Type II-rapport beoordeelt de externe auditor niet alleen het ontwerp en het bestaan van de beheersmaatregelen, maar ook de operationele effectiviteit ervan over een vooraf gedefinieerde periode van minimaal zes maanden. Dit betekent dat de externe auditor een gedetailleerd onderzoek uitvoert naar de interne controlemaatregelen van de serviceorganisatie en

nagaat of alle beheersmaatregelen effectief functioneren volgens de vooraf vastgestelde processen en controles.



Belangrijkste Voordelen

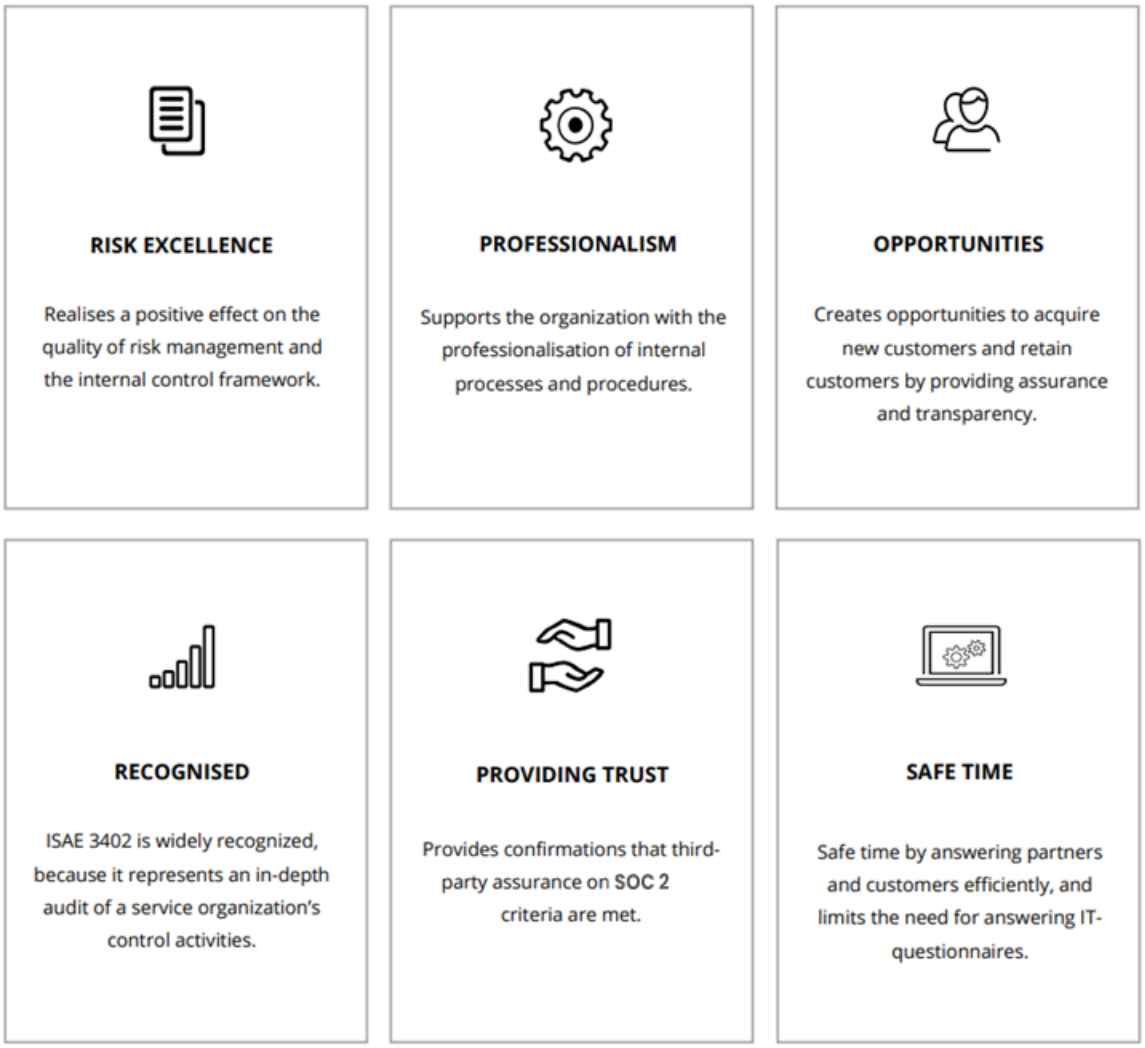
Van SOC 2 Compliance

Ervaar de voordelen van de SOC 2 Reports

SOC 2-rapporten worden door organisaties gebruikt als marketingtool. Nieuwe en bestaande klanten weten direct dat ze met een betrouwbare partij te maken hebben. Organisaties die niet over een dergelijke rapportage beschikken, lopen mogelijk belangrijke nieuwe kansen mis.

Voordeel bij inkoop

Tijdens het verkoopproces is het gebruikelijk dat een klant zijn leverancier vraagt om een IT-vragenlijst in te vullen die is opgesteld door een team van engineers. Nu zal een SOC 2-rapport waarschijnlijk effectieve antwoorden op deze vragen geven. Het zal het proces aanzienlijk versnellen. Dit zal de klant ook het gevoel en vertrouwen geven dat de processen inderdaad in orde zijn.



Kennismaken met Securance

Investeer in efficiëntie, waarde, en partnerschap

- **Analyseer risico's**
- **Plan het project**
- **Bereid systeembeschrijvingen voor**
- **Voer een gereedheidsbeoordeling uit**

Het implementeren van SOC 2 vereist zorgvuldige planning, betrokken leiderschap, een grondige analyse van processen en betrouwbare middelen en projectmanagement.

Securance is voortgekomen uit een 'Big Four'-accountantskantoor en werd opgericht in 2004. Dankzij onze achtergrond werken wij volgens de hoogste professionele standaarden en hebben wij ervaring met het behalen van strakke deadlines. Wij hanteren deze professionele standaarden in al ons werk en leveren altijd de hoogste kwaliteit, terwijl we continu streven naar het voldoen aan de behoeften van onze klanten.

Door onze platte organisatiestructuur en efficiënte communicatielijnen kunnen wij snel inspelen op uw wensen. Kiezen voor Securance betekent kiezen voor een professionele organisatie, maar ook voor een persoonlijke aanpak. Effectief projectmanagement, onze ervaring met het implementeren van risicobeheersingskaders binnen uw sector en onze professionaliteit vormen volgens ons de basis voor uitstekende resultaten.

Bij Securance geloven wij dat een goed begrip van uw organisatie, heldere communicatie en diepgaande kennis van uw sector essentieel zijn om u als klant meerwaarde te bieden. Op basis van deze aanpak houden wij u op de hoogte van relevante wetswijzigingen, regelgeving en andere belangrijke ontwikkelingen.

SECURANCE
BE SURE

Onze Tevreden Klanten

Referenties

SECURANCE
BE SURE

Securance Ltd.

63-66 Hatton Garden
London EC1N 8LE, UK
+44 20 351 446 56
www.securance.co.uk

Securance BV

Reactorweg 47
3542 AD Utrecht
+31 (0)30 2800888
www.securance.nl