

WHITEPAPER

SOC 2: waar begin je?

Een toelichting op SOC 2. Hoe begin je, hoe lang duurt het, wat kost het en waar moet je allemaal rekening mee houden?

Heldere audits. Deskundige mensen. Normaal tarief.

Inhoud

1	Introductie	3
	Wat is SOC 2?	3
	Wie beheert SOC 2?	4
	Het verschil tussen SOC 2 Type 1 en Type 2	4
	Opbouw van het normenkader	5
2	Criteria	6
	De vijf Trust Services-beginselen	6
	De criteria	6
	Points of Focus	7
	Hoe begin ik? Het proces in 12 stappen	8
3	De tijdlijnen	10
	Een planning voor SOC 2 Type 1	10
	5 manieren om je SOC 2-audit te versnellen	10
	De juiste auditororganisatie kiezen	11
4	De kosten	12

HOOFDSTUK 1

Introductie

SOC 2 is in een paar jaar tijd van nice-to-have een must-have geworden. We verwachten dat de vraag naar SOC 2-rapportages de komende jaren blijft groeien.

ISO 27001 is een goede basis voor SOC 2, maar geeft geen zekerheid (assurance). Bij een ISO 27001-audit wordt in een beperkt aantal dagen beoordeeld of de organisatie de PDCA-cyclus doorloopt. Niet alles hoeft dan al veilig te zijn, zolang je er maar van leert. Met ISO 27001 kun je aan je klanten echter niet rapporteren dat alle maatregelen in de afgelopen periode ook echt hebben gewerkt.

Dat betekent dat je in korte tijd SOC 2-expert moet worden en je bedrijf door het proces moet loodsen. En de klok tikt. Een snelle zoekopdracht laat zien dat er genoeg informatie over SOC 2 is. Sterker nog: er is heel veel. Helaas is het meeste ingewikkeld en verwarrend.

Daarom hebben we deze whitepaper gemaakt. We helpen je door de ruis heen te kijken, zodat je je kunt concentreren op wat je echt moet weten. We leggen de basisbegrippen uit, vertellen je wat je bij elke stap kunt verwachten, delen tips om je planning te verkorten en laten zien waar het echt om draait.

Wat is SOC 2?

Systems and Organization Controls 2 (SOC 2) is een auditproces dat de maatregelen van je organisatie beoordeelt. Met een SOC 2-audit laat je zien dat je voldoet aan de beveiligingseisen die klanten stellen voordat ze hun data (en vaak ook die van hun klanten) met je delen.

De kern van een assuranceopdracht zoals SOC 2 of ISAE 3402 is dat een organisatie (de gebruikersorganisatie) bepaalde diensten uitbesteedt aan een andere organisatie (de serviceorganisatie). De gebruikersorganisatie wil zeker weten dat de uitbestede dienst voldoet aan eisen op het gebied van informatiebeveiliging, juistheid, betrouwbaarheid, integriteit, vertrouwelijkheid, beschikbaarheid of privacy. Voor een rapportage over informatiebeveiliging is SOC 2 het aangewezen instrument.



Wie beheert SOC 2?

SOC 2 wordt ontwikkeld en beheerd door het American Institute of Certified Public Accountants (AICPA). Opdrachten die buiten de Verenigde Staten worden uitgevoerd, vallen niet onder de Amerikaanse wet- en regelgeving. Daarom moet uit het assurancerapport blijken dat de opdracht is uitgevoerd onder ISAE 3000 / System and Organization Controls. Het is toegestaan om op het rapport (bijvoorbeeld het voorblad) de aanduiding SOC 2® of SOC 3® te gebruiken.

Het verschil tussen SOC 2 Type 1 en Type 2

Een **Type 1** kijkt naar de maatregelen op het gebied van gegevensbeveiliging en privacy op het moment van de audit (een momentopname). Dit type rapport is minder arbeidsintensief en vormt de basis voor toekomstige audits. Het is vaak het eerste rapport dat een organisatie krijgt, omdat het het minst complex is.

Houd er rekening mee dat de meeste klanten uiteindelijk willen zien dat je je voortdurend inzet voor beveiliging en privacy. Daarvoor is een **Type 2** bedoeld. Een Type 2 kijkt naar dezelfde maatregelen als een Type 1, maar rapporteert over de werking ervan gedurende een periode van 6 tot 12 maanden, bij voorkeur een boekjaar.

	SOC 2 Type 1	SOC 2 Type 2
Wat wordt beoordeeld	Opzet en bestaan van de maatregelen	Opzet, bestaan én werking van de maatregelen
Periode	Momentopname	6 tot 12 maanden, bij voorkeur een boekjaar
Doorlooptijd	Doorgaans 1 tot 3 maanden	Doorgaans 6 tot 12 maanden
Geschikt voor	Een eerste stap en een basis voor Type 2	Aantonen dat beveiliging structureel op orde is

Opbouw van het normenkader

Een auditor heeft een normenkader nodig om te toetsen. Voor SOC 2 is dat ingewikkeld om op te stellen, al lijkt het op het eerste gezicht eenvoudig. In TSC sectie 100 van de AICPA, een lijvig document, staan alle normen. Maar niet alles is nodig: je moet een goede keuze maken, zodat alleen de relevante normen worden onderzocht.

Eerst kies je een of meer beginselen (Trust Services Criteria). Aan elk beginsel hangen criteria, en aan elk criterium hangen weer Points of Focus die de criteria verder uitwerken. Dat klinkt eenvoudig, maar uit onze ervaring met honderden SOC 2-audits blijkt dat het best complex en tijdrovend is. Het moet in één keer goed, anders verloopt het traject niet efficiënt, worden niet de juiste zaken onderzocht en sluit het rapport niet aan op wat je klanten nodig hebben.

Beginsel	Criteria	Points of Focus
Beveiliging (altijd verplicht)	33 algemene criteria (Common Criteria)	220
Beschikbaarheid	+ 3 aanvullende criteria	15
Integriteit van processen	+ 5 aanvullende criteria	19
Vertrouwelijkheid	+ 2 aanvullende criteria	4
Privacy	+ 18 aanvullende criteria	52

HOOFDSTUK 2

Criteria

De vijf Trust Services-beginselen

Het Assurance Services Executive Committee (ASEC) van de AICPA heeft categorieën en criteria opgesteld voor het beoordelen van beheersmaatregelen: de Trust Services Criteria. Ze worden van tijd tot tijd herzien; de laatste herziening was in 2022.

Beginsel	Wat het betekent
1. Beveiliging	Het systeem is beveiligd tegen ongeautoriseerde toegang, gebruik of aanpassing.
2. Beschikbaarheid	Het systeem is beschikbaar voor gebruik zoals aangegeven door de serviceorganisatie of zoals overeengekomen.
3. Integriteit van processen	De processen in het systeem zijn volledig, juist, tijdig en geautoriseerd.
4. Vertrouwelijkheid	De informatie is vertrouwelijk zoals overeengekomen.
5. Privacy	Persoonsgegevens worden verzameld, gebruikt, bewaard, verstrekt en vernietigd in overeenstemming met het privacybeleid van de organisatie en met eisen zoals de AVG.

De criteria

Een groot deel van de criteria geldt voor alle beginselen. De criteria zijn verdeeld in algemene criteria (Common Criteria), die voor alle beginselen gelden, en aanvullende criteria die voor één specifiek beginsel gelden. De algemene criteria vormen samen de volledige set voor het beginsel Beveiliging. Voor de andere vier beginselen geldt een combinatie van algemene en aanvullende criteria.

Common Criteria	Aantal	Waar het over gaat
CC1 Control Environment	5	Hoe de organisatie is ingericht: verantwoordelijkheden, integriteit, ethiek en de kwalificaties van medewerkers.
CC2 Communication and Information	3	Hoe de organisatie communiceert over beleid, processen, afspraken en verplichtingen.
CC3 Risk Assessment	4	Hoe de organisatie risico's voor haar doelstellingen identificeert en analyseert.
CC4 Monitoring Activities	2	Hoe de organisatie opzet, bestaan en werking van de maatregelen bewaakt.
CC5 Control Activities	3	Welke maatregelen de organisatie neemt om risico's te beperken.
CC6 Logical and Physical Access Controls	8	Hoe logische en fysieke toegang is beveiligd en ongeautoriseerde toegang wordt voorkomen.
CC7 System Operations	5	Hoe het systeem wordt beheerd en hoe afwijkingen en inbreuken worden gedetecteerd.
CC8 Change Management	1	Hoe wijzigingen beheerst worden doorgevoerd en ongeautoriseerde wijzigingen worden voorkomen.
CC9 Risk Mitigation	2	Hoe de organisatie reageert op risico's en het risicomanagement blijft bewaken.

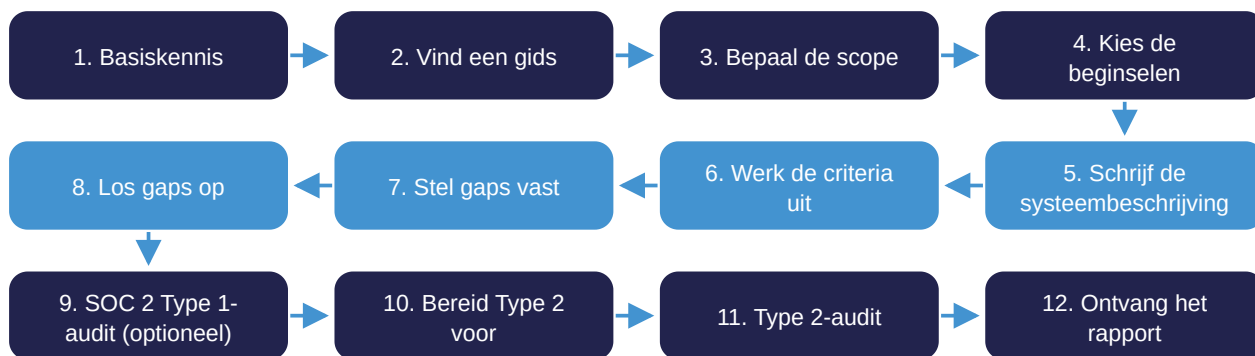
Voor Beschikbaarheid gelden 3 aanvullende criteria, voor Integriteit van processen 5, voor Vertrouwelijkheid 2 en voor Privacy 18. Meer informatie vind je op de website van de AICPA. TSC sectie 100 wordt periodiek bijgewerkt; controleer dus altijd of je de actuele versie gebruikt.

Points of Focus

In TSC sectie 100 staan onder de criteria zogenoemde Points of Focus. Ze geven voorbeelden van aandachtsgebieden waarop de serviceorganisatie met beheersmaatregelen invulling kan geven. Ze helpen de serviceorganisatie en de auditor om de belangrijkste elementen te benoemen en zorgen voor meer consistentie tussen rapporten. De Points of Focus worden niet in het rapport opgenomen. Ze zijn nadrukkelijk geen checklist: ze hoeven niet allemaal te worden geadresseerd en dienen alleen als leidraad.

Hoe begin ik? Het proces in 12 stappen

Als je nog nooit een SOC 2-traject hebt doorlopen, lijkt het ingewikkeld. Waar begin je? Wat zijn de stappen? Wie doet wat? Hieronder het proces in een notendop.



1 Basiskennis

Leer de basis, maar ga niet te diep in op de details. Deze whitepaper doorlezen is een goede eerste stap: je krijgt een beeld van het auditproces, het bepalen van de scope en het opstellen van een plan van aanpak.

2 Vind een gids

Tenzij je eerder een SOC 2-audit hebt doorlopen, heb je begeleiding nodig. Wij kunnen je als auditor begeleiden. Je kunt ook een consultant inhuren of investeren in software die de workflow automatiseert. Wij hebben alles in huis om je van begin tot eind te ondersteunen, zodat de juiste stappen worden gezet, effectief en efficiënt.

3 Bepaal de scope

Bepaal samen met ons de scope van de SOC 2-rapportage. Voor welke dienstverlening wil je de verklaring hebben, welke locaties vallen erbinnen en welke technologieën?

4 Kies de beginselen

Stel vast welke beginselen onderzocht moeten worden. Beveiliging is altijd verplicht. Welke andere criteria vraagt je klant, of passen bij je dienstverlening? Ook hierbij helpen we je een goede keuze te maken.

5 Schrijf de systeembeschrijving

Sectie 3 van het SOC 2-rapport is een beschrijving van het zogenoemde systeem: de scope en gekozen beginselen, maar ook je organisatie, dienstverlening, IT-componenten, uitbestede diensten, HR-beleid en interne beheersing. Hiervoor gebruiken we templates op basis van de richtlijnen van de AICPA.

7 Stel gaps vast

Als het normenkader, de scope, de beginselen en de beschrijving klaar zijn, volgt een gapanalyse. We lopen het normenkader met je door om op hoofdlijnen vast te stellen waar je al aan voldoet. Houd deze stap eenvoudig: het doel is om hiaten vroeg te zien, zodat je tijd hebt om ze vóór de audit op te lossen.

9 SOC 2 Type 1-audit (optioneel)

Een Type 1 is een tussenstap naar een Type 2. Zo laat je je klanten al zien dat je een belangrijke eerste stap hebt gezet. Het is een mooie afronding van de voorgaande stappen en een goede voorbereiding op de Type 2: we kunnen dan al aangeven welk bewijsmateriaal nodig is om de werking vast te stellen.

11 SOC 2 Type 2-audit

Na afloop van de periode voeren we de audit uit. De auditor controleert per norm de documentatie, processen en procedures (opzet), of er ook zo wordt gewerkt (bestaan) en of dat gedurende de hele periode aantoonbaar zo is gebeurd (werking).

6 Werk de criteria uit

Een lastige stap: de criteria zijn vrij algemeen beschreven. De Points of Focus geven richting, maar ga niet te ver in de details. We hebben een mapping naar ISO 27001, waardoor je snel ziet welke criteria al zijn geïmplementeerd. Al onze auditors zijn lead auditor ISO 27001 en kennen beide werelden.

8 Los gaps op

Op basis van de gapanalyse los je de hiaten op, zodat ze vóór de audit zijn weggewerkt. De doorlooptijd hangt af van het aantal gaps en van de complexiteit en omvang van je organisatie.

10 Bereid de Type 2 voor

In de periode daarna ligt de nadruk op het structureel verzamelen van bewijsmateriaal, zodat je kunt aantonen dat de maatregelen de hele periode hebben gewerkt. Eventueel voeren we tussentijds een controle uit om te zien of alles op de juiste manier gebeurt.

12 Ontvang het rapport

De laatste stap is het uitbrengen van de rapportage en het afgeven van de verklaring. Die kun je delen met je klanten.

Tip: heb je al een ISO 27001-certificaat? Dan heb je een goede basis. Met onze mapping zie je snel welke SOC 2-criteria al zijn afgedekt en waar nog werk ligt.

HOOFDSTUK 3

De tijdlijnen

Een SOC 2 Type 1-audit duurt doorgaans één tot drie maanden. Een SOC 2 Type 2-audit duurt tussen de zes en twaalf maanden.

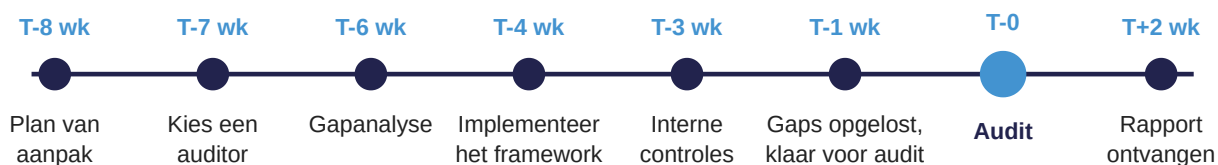
Een exacte doorlooptijd is lastig te geven. Elke organisatie is uniek en SOC 2 is een flexibel framework zonder vaste regels. Elke organisatie heeft een ander vertrekpunt, kiest andere beginselen en interpreteert ze op haar eigen manier. Op basis van onze ervaring met honderden SOC 1- en SOC 2-trajecten kunnen we wel grove uitgangspunten geven.

Waar hangt de doorlooptijd van af?

- De grootte van je organisatie
- De volwassenheid van je bestaande processen en beleid
- Het aantal mensen dat bij het proces betrokken is
- Het aantal criteria dat je opneemt
- De mate van betrokkenheid van het management

Een planning voor SOC 2 Type 1

Met inzicht in de tijdlijn, een harde deadline en een planning waarin je terugreken en per activiteit een datum vastlegt, houd je het proces op schema. Hieronder een voorbeeldplanning richting een SOC 2 Type 1-rapportage (T-0 is de audit).



5 manieren om je SOC 2-audit te versnellen

1. **Doe het niet alleen.** Zeker de eerste keer heb je expertise aan je zijde nodig, van auditors tot je interne team.
2. **Wees eerlijk.** Verdoezel je zwakke punten bij de gapanalyse, dan struikel je tijdens de audit en loop je vertraging op.
3. **Zoek zo snel mogelijk een auditor.** Wacht niet tot de voorbereiding klaar is: de auditor helpt je juist bij de beste aanpak.
4. **Maak een planning.** Leg een deadline vast en reken terug. Zo weet iedereen wat er moet gebeuren en wat zijn rol is.
5. **Zorg voor steun van het management.** HR, IT, legal en finance doen mee. Zonder steun van bovenaf verliest het project snelheid.

De juiste auditororganisatie kiezen

Het implementeren en documenteren van de maatregelen is een van de meest intimiderende en tijdrovende onderdelen van SOC 2. De AICPA biedt weinig houvast over welke maatregelen je moet invoeren of hoe je ze in het rapport beschrijft. Zonder voorbeeld is het lastig om de bal aan het rollen te krijgen. Daar kan Auditvision helpen.

Bij SOC 2 kies je zelf wie je werk beoordeelt. Die keuze is belangrijk: de auditor beslist of je een schoon rapport krijgt én helpt je door een complex proces. Deze tips helpen je bij de keuze.

1 Zoek flexibiliteit

Er is niet één juiste manier om SOC 2 te implementeren. Kies een auditor die de eigenheid van je bedrijf in het normenkader kan verwerken. Sommige auditors werken met een one-size-fits-all-proces; wij kiezen voor samenwerking, met heldere templates waar dat helpt.

3 Let op de sfeer

Belangrijker dan de contractuele verplichtingen is een open, samenwerkende aanpak. Flexibiliteit en wederzijds respect voorspellen het succes beter dan het contract.

5 Denk aan je interne team

Veel bedrijven die een SOC 2-audit nodig hebben, hebben al snel meer dan 25 medewerkers. Zorg dat het interne team kennismaakt met de auditor om te zien of de samenwerking klikt.

7 Praat met het deliveryteam

Verkopers vertellen wat je wilt horen, maar zijn na het tekenen niet je aanspreekpunt. Praat rechtstreeks met het deliveryteam en de teamleider.

2 Maak duidelijke afspraken

Heb je afspraken met klanten, stem de planning dan af met de auditor. Weet de auditor wat hij van jou nodig heeft, zoals de scope, de uitwerking van de Points of Focus en het bewijsmateriaal? Wij nemen regelmatig projecten over waarbij die kennis ontbrak, ook bij grote kantoren.

4 Werk samen

Bij een eerste SOC 2-audit zien organisaties de auditor vaak als de baas. Maar jij bent de baas: zet de agenda, daag de auditor uit en vraag hem je halverwege tegemoet te komen.

6 Kies het team, niet het merk

Kies je auditor niet op de bekendheid van de naam. Een merk bestaat uit veel teams; alleen het team dat met jou samenwerkt, telt.

8 Vraag om referenties

Vraag altijd om referenties van organisaties die qua grootte, branche en situatie op de jouwe lijken.

HOOFDSTUK 4

De kosten

Een SOC 2-traject bij AudITvision kost voor een organisatie met minder dan 25 medewerkers ongeveer € 10.000, inclusief begeleiding. In de jaren daarna nemen de kosten af.

Klanten vragen ons vaak vooraf wat een SOC 2-audit kost. Dat begrijpen we, ook omdat we soms bedragen horen die echt niet realistisch zijn. Een eenduidig antwoord is lastig, maar op basis van de honderden audits die we hebben uitgevoerd, kunnen we wel richtlijnen geven.

We gaan hierbij uit van een klant die alleen het beginsel Beveiliging heeft gekozen. Dat is verplicht en ook het meest omvangrijke beginsel. We rekenen met een uurtarief van € 150. Veel kantoren hanteren een veel hoger tarief en brengen nog allerlei andere kosten in rekening.

De bedragen hieronder zijn inclusief alle stappen, dus niet alleen de audit. Bij een Type 1 gaat veel tijd naar begeleiding; bij een Type 2 gaat veel tijd naar het beoordelen van het bewijsmateriaal. Na de eerste Type 2 neemt de inspanning in de jaren daarna af.

Aantal medewerkers	Type 1	Type 2	Volgende jaren
Minder dan 25	€ 10.000	€ 10.000	€ 8.000
25 tot 100	€ 15.000	€ 15.000	€ 12.000
100 tot 250	€ 25.000	€ 25.000	€ 20.000
250 tot 1.000	€ 27.500	€ 35.000	€ 25.000
Meer dan 1.000	op aanvraag	op aanvraag	op aanvraag

Indicatieve bedragen, exclusief btw, uitgaande van het beginsel Beveiliging.

Vragen over SOC 2?

We denken graag met je mee over de scope, de planning en de kosten van jouw SOC 2-traject.

T 088-2028700

E info@auditvision.nl

W www.auditvision.nl

Heldere audits. Deskundige mensen. Normaal tarief.