TOPCERTIFIER
www.topcertifier.com

SERVICEMETHODOLOGIE VOOR SOC Certificering

CONTROLE VAN DE DIENSTORGANISATIE

TOPCERTIFIER
www.topcertifier.com

Wat zijn SOC-rapporten?

SOC-rapporten zijn een manier voor bedrijven om dit via een onafhankelijke derde partij te verifiëren dienstverleners beschikken over passende controles en volgen voorheen de industrienormen het uitbesteden van een bedrijfsfunctie aan die organisatie. Dit biedt dienstverleners kansen om geloofwaardigheid te creëren en vertrouwen op te bouwen bij klanten, investeerders, zakenpartners en auditors terwijl u een concurrentievoordeel op de markt verkrijgt. Alle SOC onderzoeken worden uitgevoerd volgens

AICPA-richtlijnen:

Tijdens het proces van **SOC-implementatie** een ervaren team van technologieconsultants en auditors zullen nauw samenwerken met de leiding van uw organisatie om ervoor te zorgen dat:

- Het uiteindelijke SOC-rapport wordt grondig en tijdig afgestemd op de unieke behoeften van een organisatie
- Bedrijfsactiviteiten en interne controleprocessen zijn gestroomlijnd
- Er wordt voldaan aan contractuele verplichtingen en zorgen op de markt
- Er wordt voldaan aan de AICPA-rapportagevereisten

Hoe bepaal ik het type SOC-rapport Mijn zakelijke behoeften?

Er zijn twee belangrijke redenen om een SOC-beoordeling en certificering te ondergaan:

- Een (potentiële) klant of auditor vraagt om een SOC-rapport
- Uw organisatie besluit proactief soc-compliance te verdienen

In het eerste scenario zou de aanvrager waarschijnlijk het benodigde type SOC-rapport kunnen specificeren. In beideln dit scenario moet een organisatie eerst nadenken over haar doelstellingen. Meestal het gewenste resultaat voor iedereenDe organisatie moet aantonen dat zij zich inzet voor een passend ontwerp en een effectieve werkingvan zijn interne controleomgeving.

TOPCERTIFIER
www.topcertifier.com

Vergelijkingstabel SOC 1, 2 en 3

Er zijn drie verschillende typen SOC-rapporten: SOC 1, SOC 2 en SOC 3. Elk rapport varieert, maar biedt waardevolle informatie die nodig is om de risico's en de daarmee samenhangende interne controles te beoordelenmet een externe dienstverlener. Voor het onderzoek is een onafhankelijke, externe auditor nodigen bevestig verschillende aspecten van een organisatie voordat het eindrapport wordt opgesteld.

SOC 1	SOC 2	SOC 3
Rapporteer over uw interne controles die verband houden met financiële zakeninformatie of verklaringen	Rapporteer over uw interne controles gerelateerd aan vijf vertrouwensdiensten principes: veiligheid, beschikbaarheid, integriteit, vertrouwelijkheid en privacy	Verslag over de resultaten vanSOC 2 op een geschikte manier voor publiek publiek.
Meestal gedeeld met auditors	Meestal gedeeld met klanten en belanghebbenden	Gedeeld voor het grote publiek
Van toepassing op bedrijven welk proces financieel informatie zoals medische gegevens Claimverwerking, salarisadministratie Diensten, kredietverstrekkers enz	Toepasbaar voor elk technologiebedrijfdat gaat over informatieverwerking. Zowel product- als servicegericht bedrijven	Toepasbaar voor ieder publiekonderneming die beschikt over eenSOC 2 geverifieerd en gewenst om een SOC 3-rapport te produceren voor een groter publiek publiek

TOPCERTIFIER
www.topcertifier.com

SOC 1 CERTIFICERING

Een SOC 2-rapport richt zich op de controles van uw organisatie die relevant zijn voor de financiële situatie van een gebruikersorganisatie rapportage. Het is een hypergedetailleerd onderzoek dat een gespecialiseerd begrip vereist van deindustrie en de daarmee samenhangende controleomgeving. Meestal specificeert de serviceorganisatie haar controledoelstellingen en daarmee samenhangende controleactiviteiten op basis van de specifieke diensten die zij verrichten.

Een SOC 1-rapport bevat over het algemeen bedrijfsprocescontroles waarbij de uitvoering betrokken is. Een SOC 1 rapport omvat over het algemeen bedrijfsprocescontroles die betrekking hebben op de volledigheid en nauwkeurigheid van transacties, evenals algemene informatietechnologiecontroles, zoals netwerkbeveiliging en logische toegang.

Gezien de beperkte reikwijdte is een SOC 1-rapportage het meest geschikt voor organisaties die moeten inboezemenvertrouwen in hun controles en waarborgen met betrekking tot de financiële gegevens van hun klanten. Het is vaaknoodzakelijk wanneer de gebruikersorganisatie openbaar wordt verhandeld en moet voldoen aan SOX 404 of iets dergelijksregelgeving. Hier zijn enkele voorbeelden:

Administratie Diensten

Medische claims verwerking

Payrolldiensten

Uitleendiensten

TOPCERTIFIER
www.topcertifier.com

SOC 2 CERTIFICERING

Een SOC 2-rapport is bedoeld voor serviceorganisaties waarvan de gebruikersentiteiten niet noodzakelijkerwijs reageren controles voor financiële rapportage, waardoor aanbieders kunnen voldoen aan de behoeften van een breder scala aan bedrijven gebruikersentiteiten.

Een SOC 2-onderzoek richt zich vooral op de manier waarop gegevens worden opgeslagen en beschermd controles met betrekking tot de serviceverplichtingen en systeemvereisten op basis van de AICPA's criteria voor vertrouwensdiensten (hieronder gedefinieerd).

- **Beveiliging** – Informatie en systemen zijn beschermd tegen ongeoorloofde toegang en openbaarmaking van informatie

- **Beschikbaarheid** – Informatie en systemen zijn beschikbaar voor bediening en gebruik om aan de eisen van de entiteit te voldoen doelstellingen

- **Verwerkingsintegriteit** – De systeemverwerking is compleet, geldig, accuraat, tijdig en bevoegd om de doelstellingen van de entiteit te verwezenlijken

- **Vertrouwelijkheid** – Informatie die als vertrouwelijk is aangemerkt, wordt beschermd om te voldoen aan de eisen van de entiteit doelstellingen

- **Privacy** – Persoonlijke informatie wordt verzameld, gebruikt, bewaard, openbaar gemaakt en ter beschikking gesteld de doelstellingen van de entiteit

SOC 2-rapporten kunnen worden gebruikt door elk technologiebedrijf dat zich bezighoudt met informatieverwerking. Terwijl SOC 1- en SOC 2-rapporten beide een beperkt publiek hebben, rapporteert SOC 2kan aan andere partijen worden gegeven, zoals potentiële klanten en leveranciersbeheer professionals, toezichthouders en andere belangrijke zakenpartners.

TOPCERTIFIER
www.topcertifier.com

SOC 3 CERTIFICERING

Net als SOC 2 richten de SOC 3-rapporten zich op controles die relevant zijn voor de vijf vertrouwensdiensten van de AICPA categorieën. In tegenstelling tot SOC 2 zijn SOC 3-rapporten echter gecertificeerd en kunnen ze openbaar worden gemaakt beschikbaar, waardoor ze waardevolle hulpmiddelen zijn voor het op de markt brengen van de effectiviteit van uw controle omgeving.

Indien u een SOC 3-rapport wenst, dient uw organisatie eerst een SOC 2, Type 2 in te vullen onderzoek (meer over rapporttypen hieronder). SOC 2 en SOC 3 onderzoeken kunnen worden uitgevoerd op een of meer van de categorieën vertrouwensdiensten. SOC 3-rapporten bevatten veel van hetzelfde informatie opgenomen in SOC 2-rapporten, behalve met een veel minder gedetailleerde beschrijving van uw controles met betrekking tot compliance en bedrijfsvoering. Ze omvatten ook geen specifieke controle activiteiten, testprocedures of gedetailleerde resultaten over de operationele effectiviteit.

TYPE 1 versus TYPE 2

Alle SOC-rapporten (behalve SOC 3) kunnen van Type 1 of Type 2 zijn. Het verschil is voornamelijk gebaseerd op de reikwijdteperiode

- **Type 1 rapport :** EEN TYPE 1 RAPPORT beschrijft de geschiktheid van de serviceorganisatie voor de ontwerp en implementatie van controles op een specifiek tijdstip

- **Type 2 rapport :** EEN TYPE 2 RAPPORT zorgt ervoor dat gedefinieerde controleactiviteiten consistent zijneffectief werkend gedurende een bepaalde periode, die gewoonlijk 6 maanden tot 1 jaar bedraagt, waardoor betere operationele prestaties worden behaald

In veel gevallen zal een serviceorganisatie beginnen met een Type 1-rapport om de beheersing te definiëren activiteiten, vanaf een bepaald moment. Zodra de bedieningselementen zijn ontworpen en geïmplementeerd, is de Type 2 de rapport zou volgen. Omdat het Type 2-rapport een periode bestrijkt (d.w.z. 6 of 12 maanden), is dit rapport waardevoller voor gebruikers omdat het verzekert dat er gedurende een bepaalde periode controles hebben plaatsgevonden effectief. Een organisatie schakelt doorgaans een accountantskantoor in om het Type 2-rapport in te vullen. jaarlijks.

TOPCERTIFIER
www.topcertifier.com

Hoe bereid ik me voor op een SOC-beoordeling?

Bij het starten van uw eerste SOC-beoordeling is het voordelig om samen te werken met de door u geselecteerde derde partijeen consultant zoals wij om een initiële gap-analyse uit te voeren, zodat u eventuele hiaten kunt verhelpenvóór de start van het SOC-rapportageproces. Door deze route te volgen, kun je het bestaande vullen gaten in uw huidige systeem, waardoor een veel conformer systeem ontstaat dat heel dichtbij is om aan de SOC-vereisten te voldoen. Hoewel elk SOC-rapport een andere reikwijdte heeft, zijn er bepaalde aandachtsgebieden die essentieel zijn voor alle SOC-beoordelingen. Door zich te concentreren op de volgende taken, kan een organisatie kan beginnen met het voorbereiden van haar medewerkers op een sterkere controleomgeving dus een efficiëntere SOC-beoordeling.

DOCUMENTATIE

Vanuit het perspectief van een auditor: als het niet gedocumenteerd is, bestaat het niet. Alhoewel dat mag Als er sterke interne controles zijn, wordt het bewijs van een gebeurtenis mogelijk niet herdacht. Ervoor zorgenEr wordt documentatie bijgehouden ter ondersteuning van alle bestaande controles (bijvoorbeeld goedkeuring voor toegangsverlening,erkenningen van werknemers, onderhoud van populaties, enz.).

GEDEFINIEERD BELEID EN PROCEDURES

Om ervoor te zorgen dat alle relevante partijen hun verantwoordelijkheden begrijpen om aan de organisatorische verplichtingen te voldoendoelstellingen, ervoor te zorgen dat fundamentele processen en procedures worden gedocumenteerd. Dit levert een hulpmiddel voor zowel medewerkers als auditors om de intentie van de organisatie binnenin te begrijpen de controleomgeving. De reikwijdte van het beleid moet het volgende omvatten:

» Organisatorische procedures om aan contractuele verplichtingen te voldoen

» Middelen om te voldoen aan de belangrijkste serviceverplichtingen en systeemvereisten

» Risicobeheer aanpak

RISICOBEOORDELING

Een geformaliseerd proces, gefaciliteerd door een jaarlijkse risicobeoordelingsbespreking en goedgekeurd door deraad van bestuur of uitvoerend management moet bestaan. In plaats van een formeel jaarlijks risicoBij een evaluatie kan een organisatie er ook voor kiezen om driemaandelijks bijeenkomsten te houden om veranderingen in de bedrijfsvoering te bespreken bedreigingen, bedrijfsactiviteiten, enz., en hun impact op de algehele risicobeoordeling. Het risico De beoordeling moet gedefinieerde risiconiveaus (d.w.z. lage, gemiddelde en hoge dreiging) omvattenDe herstelaanpak van het bedrijf (d.w.z. accepteren, beperken of elimineren) met details over hoe deHet bedrijf heeft gereageerd of is van plan in de toekomst te reageren.

TOPCERTIFIER
www.topcertifier.com

SOC-implementatieroutekaart

Hoewel elk SOC-rapport verschillende vereisten en doelstellingen heeft, wordt elk rapport over het algemeen uitgevoerd volgende zeven hoofdfasen

	PROCESFASE	BELANGRIJKSTE DEELNEMERS	BELANGRIJKSTE MATERIALEN
1	Scoren	Topmanagement Accountants, adviseur	Achtergrondinformatie over organisaties behoeften en klantwensen
2	Doorloop nl Controle ontwerp	Adviseur, Proceseigenaren	Bestaand beleid en procedures, materialen van de tijd die met elke proceseigenaar wordt doorgebracht
3	Beoordeling van de kloof	Adviseur, Proceseigenaren	Preliminary documentation to support remediation roadmap
4	Sanering	Adviseur, Proceseigenaren	Documentation for validation of the control environment
5	Examen testen	Auditor, adviseur, proces Eigenaren	Procesdocumentatie, examen bewijsmateriaal
6	Rapport	CPA-auditoren	Beleid en procedures, conceptfeedback, reactie op feedback en uitzonderingen
7	Uitgifte	CPA-auditoren	SOC-rapport

Zelfs bij eerstejaarsexamens kunnen de meeste fasen binnen een bepaalde tijd worden doorlopen De tijdlijn, hoewel de meest onvoorspelbare van de fasen, is herstel (fase 4).Op basis van de resultaten van de kloof wordt het niveau van de inspanningen voor herstel bepaaldbeoordeling (fase 3). Tijdens de beoordelingsfase zorgt uw accountantskantoor voor een herstelmaatregel routekaart om naleving van de toepasselijke SOC-criteria te garanderen. Door een sterke controle te creëren omgeving vóór aanvang van het examen leg je de basis voor een georganiseerde, minimaal verstorende audit.

TOPCERTIFIER
www.topcertifier.com

SOC-auditdiensten

Ons ervaren team ondersteunt serviceorganisaties over AICPA SOC-rapportagevereisten.Wij bied waardevolle informatie die klanten, prospects en auditors nodig hebben om te hebben beoordeelde risico's en interne controles die verbonden zijn aan een uitbestede belangrijk.

Als gekwalificeerd adviesbureau op dit gebied hebben we talloze gesprekken gevoerd onderwijs, waarde en efficiëntie. Wij zijn er trots op dat we samenwerken met organisaties die specifieke doelstellingen hebbenbehoeften, concurrerende prioriteiten, tijdsdruk en andere unieke doelstellingen. Wij begrijpen de waarde van tijd, passende planning en opleiding die een naadloos examen garanderenvordert.

Over TOPCertificator

TOPCertifier is een wereldwijd erkend managementadviesbureau gespecialiseerd in informatie veiligheidsdiensten en soc-beoordelingen.

Het hoofdkantoor is gevestigd in Bangalore (India) en we hebben vestigingen in meer dan 20 landen met een specialiteit focus op de VS, Europa en de Golfstaten. We hebben ook een indrukwekkende aanwezigheid in Azië-Pacifische en Afrikaanse regio's. We hebben ruim 2.800 organisaties geadviseerd, verspreid over een groot aantal industrieën, op het gebied van boekhouding, belastingen, winstgevendheid en bedrijfsprocesoplossingen, sinds onze oprichting in januari 2010. Met een team van meer dan 200 branchedeskundige adviseurs, gecertificeerde hoofdauditors en Subject Matter Experts, we hebben een track record van 100% geleverd wat betreft onze certificering succespercentage .

Bedankt

OM MEER TE LEREN,

BEZOEK WWW.TOPCERTIFIER.COM