SECURANCE

Vitpapper - SOC 2

SOC 2 Efterlevnad.

SOC 2 Efterlevnad

Outsourcing | Trust Services Criteria

SOC 2 är en rapport enligt Service Organization Control (SOC) som ger säkerhet över outsourcade processer. En revision som utförs i enlighet med SOC 2 är allmänt erkänd eftersom den representerar en djupgående granskning av en tjänsteorganizations kontrollaktiviteter, som inkluderar kontroller över intern kontroll, säkerhet, riskhantering och relaterade processer. SOC 2-rapporter utarbetas i enlighet med Trust Services Criteria.

SOC 2 fokuserar på en verksamhets icke-finansiella rapporteringskontroller i relation till säkerhet, tillgänglighet, bearbetningsintegritet, konfidentialitet och integritet. Dessa principer är angivna i Trust Services Criteria. Varje kriterium har definierade krav (Points of Focus) som måste uppfyllas och implementeras inom organisationen för att visa efterlevnad av kriterierna.

Modulär

SOC 2-rapporter är modulära, vilket innebär att rapporterna kan täcka ett eller flera av principerna beroende på en tjänsteorganisations behov och krav. Det enda kriteriet som är obligatoriskt för SOC 2 är säkerhetskriteriet. Dessa kriterier kallas också för de gemensamma kriterierna.

Gemensamma Kriterier

Det enda kriteriet som är obligatoriskt för SOC 2 är säkerhet, vilket även kallas de Gemensamma Kriterierna. Ytterligare kriterier kan inkluderas inom ramen för en SOC 2-rapport.

Förutom säkerhetskrav (logiska och fysiska åtkomstkontroller, systemoperationer och förändringshantering) innehåller de Gemensamma Kriterierna också krav på ett internt kontrollramverk, inklusive riskhantering (COSO). De viktigaste elementen i COSO-ramverket är Kontrollmiljö, Kommunikation och Information, Riskbedömning och Riskhantering, Övervakningsaktiviteter och Kontrollaktiviteter.

De valda kriterierna implementeras inom organisationen och redovisas i SOC 2-rapporten genom att följa punkterna för fokus och ytterligare kriterier enligt COSO 2013 (riskhantering) ramverket och Trust Services Criteria. Därefter granskas SOC 2-rapporten av oberoende revisionsbyråer.

Trust Services Criteria

Kriteriernas Beskrivning

Det enda obligatoriska kriteriet är säkerhetskriteriet, som tidigare har beskrivits. Oftare övervägs tillämpligheten av kriterierna för tillgänglighet, konfidentialitet, bearbetningsintegritet och integritet baserat på de tjänster som erbjuds, samt i samråd med nyckelkunder och SOC 2-experter. När en organisation väljer att inkludera kriterier måste alla tillhörande krav och fokusområden beaktas och implementeras när det är tillämpligt. Nyckelkarakteristika för varje kriterium beskrivs nedan.

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.

FAS 1. OMFÅNGSDEFINITION

Hur man Definierar Omfånget av en SOC 2-rapport

Omfånget för en SOC 2-rapport avser de (icke-finansiella) kontroller inom en tjänsteorganisation som är relevanta för säkerhet, tillgänglighet, bearbetningsintegritet, konfidentialitet och/eller integritet, vilka definieras i Trust Service Criteria. SOC 2-rapporten bör innehålla en avsnittsdel som beskriver de viktigaste komponenterna i omfånget. Det är nödvändigt att inkludera detaljer om vilken/vilka typer av tjänster som tillhandahålls samt infrastruktur, mjukvara, personal, policys och procedurer, och data som är relevanta för dessa tjänster.

Exempel

För en leverantör av Software as a Service (SaaS) är deras omfång vanligtvis deras mjukvaruapplikation(er) som är tillgänglig(a) för deras kunder. Detta inkluderar all data som lagras i systemet, infrastrukturen som värd för det, och de personer och procedurer som stödjer det. Underleverantörer och kompletterande kontrollområden för användarenheten ger ytterligare detaljer om omfånget i andra avsnitt av rapporten genom att definiera gränserna för omfånget inom rapporten.

Slutsats

I slutändan är det upp till ledningen att definiera omfånget för en SOC 2-rapport. Kontroller som fokuserar på tjänsteorganisationens verksamhet och som är väsentliga för organisationens icke-finansiella rapporter måste inkluderas i omfånget. Förutom att omfånget måste vara tydligt definierat och redovisat i rapporten, finns det viss flexibilitet. Ansvaret för att säkerställa att rapporten uppfyller slutanvändarnas krav ligger hos ledningen.

Konkurrensfördel

Hur en SOC 2-Rapport Ger Dig ett Försprång Över Dina Konkurrenter

SOC 2 ger en konkurrensfördel genom att skilja tjänsteorganisationer från deras konkurrenter. Fördelarna med SOC 2-rapporter omfattar förbättring och finslipning av riskhantering, samtidigt som marknadens förtroende främjas genom en transparent presentation av kontrollramverket. Implementeringen av SOC 2 ökar revisionseffektiviteten och minskar operativa ineffektiviteter inom verksamheten.

FAS 2. Implementering

Steg-för-steg-metod

1. Påverkansanalys & Omfattning

I fas 1 fastställs påverkan (GAP-analys) av implementeringen och tillämpligheten av Trust Services Criteria bedöms. Baserat på påverkan och den definierade omfattningen av implementeringen utarbetas en detaljerad plan där olika milstolpar identifieras och överenskommelser görs med ledningen.

2. Processer & Kontroller

I fas 2 hålls intervjuer för att identifiera risker, fastställa påverkan och den befintliga arbetsmetoden samt ta del av information som finns inom organisationen. Organisationens kontrollåtgärder beskrivs sedan enligt SOC 2-kraven baserat på den information som erhållits från intervjuerna. Dessa registreras i en kontrollmatris, en matris som innehåller SOC 2-kraven och relaterade kontrollåtgärder. Vi kommer att ge proaktiv rådgivning om implementeringen av eventuella saknade kontroller (inklusive processbeskrivningar).

3. Kontrollramverk

I fas 3 kommer Securance att beskriva kontrollramverket baserat på det senaste COSO-ramverket (COSO 2013) och förbereda den allmänna delen av rapporteringen. I den allmänna delen ingår en beskrivning av processerna, organisationen och de allmänna IT-kontrollerna.

4. SOC 2-Rapport

I fas 4 förbereds den fullständiga SOC 2-rapporten baserat på de individuella avsnitten och ytterligare avsnitt såsom ledningens uttalande och kompletterande användarkontroller. Fas 4 resulterar i ett utkast till SOC 2-rapport. Vi kommer att diskutera denna rapport i detalj med relevant personal. Organisationen kommer att implementera eventuellt identifierade saknade kontroller under denna fas. Behandlingstiden för de första fyra faserna kommer att vara mellan sex och åtta veckor, beroende på de anställdas engagemang och tillgänglighet. Den förväntade tillgängligheten för anställda är en dag per vecka under denna period.

5. Förrevision

Efter att rapporten har förberetts kommer Risklane att genomföra en förrevision eller 'genomgång' i fas 5. Under förrevisionen kommer kontrollåtgärder att testas, och eventuella problemområden kommer att identifieras före den slutliga revisionen. Under denna fas kommer organisationen att tillhandahålla den dokumentation och de bevis som krävs av Risklane.

6. Återställning

Under fas 6, som ett resultat av förrevisionen, implementeras förbättringar av kontrollåtgärder och ledningssystemet, och lösningar för de identifierade problemområdena förbereds. Securance kommer att tillhandahålla lösningar som kan implementeras inom organisationen och i SOC 2-rapporten. Fas 6 kommer att resultera i den slutliga SOC 2-rapporten.

Behandlingstiden för faserna 5 och 6 är mellan två och fyra veckor. Den förväntade tillgängligheten för anställda är en dag per vecka under denna period.

FAS 3. Revisionen

Kvalitetssäkringsrevisioner

SOC 2-Revisionerna Förklaras

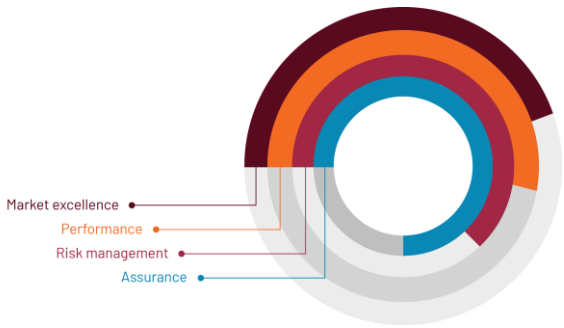
Nyckeln till framgångsrik outsourcing är att välja en tjänsteleverantör som förstår din organisation. En SOC 2-certifiering ger en garanti för säkerheten, tillgängligheten, konfidentialiteten, bearbetningsintegriteten och integritetsskyddet av information. Om du hanterar känsliga kunduppgifter är dessa element avgörande framgångsfaktorer. I en SOC 2-rapport beskrivs riskkontrollramverket, inklusive de relaterade kontrollerna och procedurerna för att övervaka riskkontrollramverket. Rapporten utarbetas i enlighet med Trust Services Criteria för att tillhandahålla ett uppsättning kriterier för säkerhet, tillgänglighet, bearbetningsintegritet och integritetsskydd för att hålla jämna steg med den snabba tillväxten av molntjänster och utmaningar inom affärsoutsourcing som den globala ekonomin innebär.

Type I Rapport

En SOC 2 Typ I-rapport inkluderar ett yttrande från en extern revisor om de kontroller som har implementerats vid en specifik tidpunkt. Den externa revisorn undersöker huruvida kontrollerna är lämpligt utformade för att ge rimlig säkerhet att de finansiella rapporteringspåståendena uppfylls och om kontrollerna är på plats.

Type II Rapport

I en SOC 2 Typ II-rapport redogör den externa revisorn för lämpligheten av designen och förekomsten av kontroller samt för kontrollernas operativa effektivitet under en fördefinierad period på minst sex månader. Detta innebär att den externa revisorn utför en detaljerad granskning av tjänsteorganisationens interna kontroll och undersöker även om alla kontroller fungerar effektivt i enlighet med de fördefinierade processerna och kontrollerna.



Viktiga Fördelar

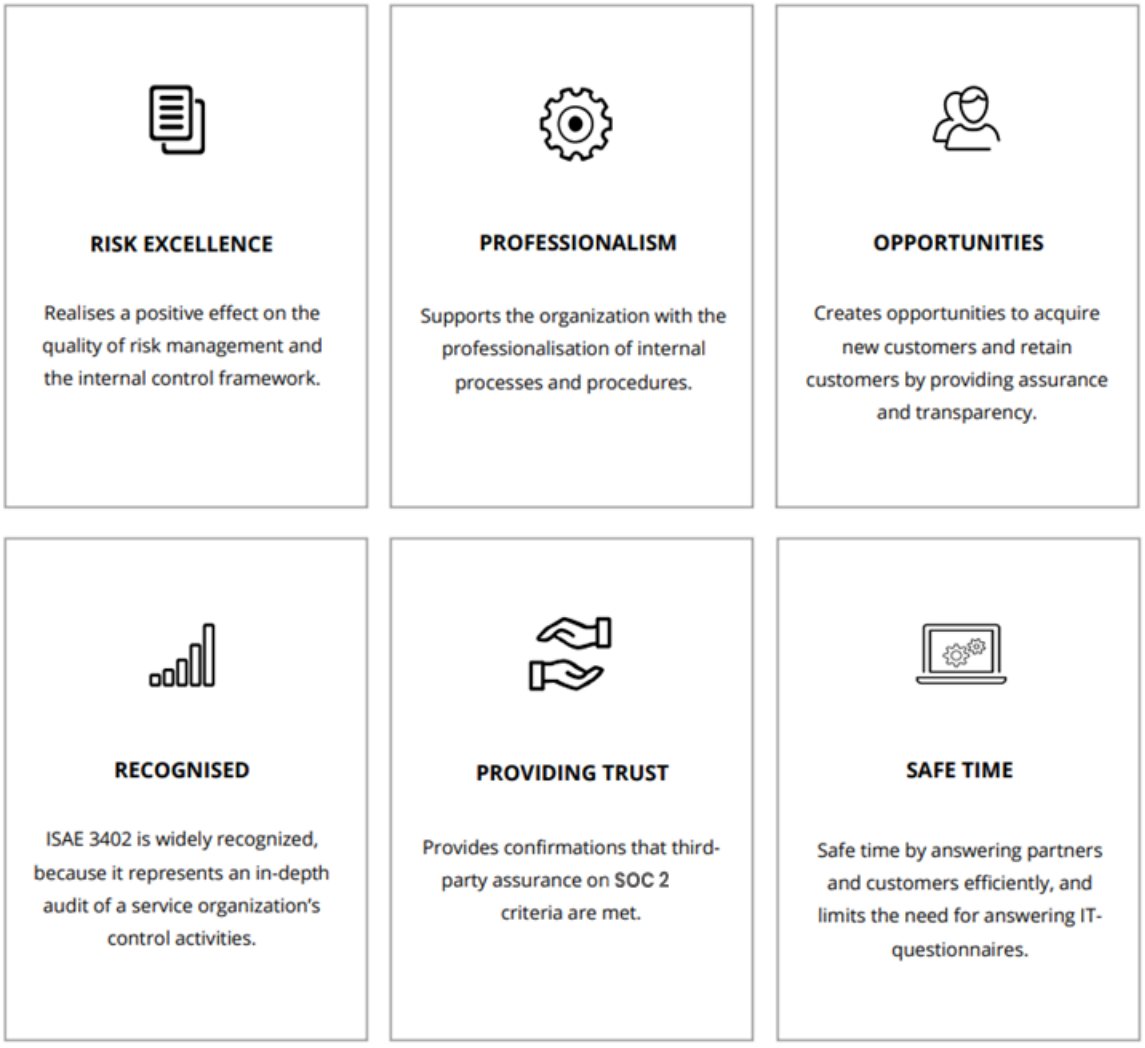
Med SOC 2-Efterlevnad

Upplev fördelarna med SOC 2-rapporter

SOC 2-rapporter används av organisationer som ett marknadsföringsverktyg. Nya och befintliga kunder vet omedelbart att de har att göra med en pålitlig partner. Organisationer som inte har sådana rapporter kan gå miste om viktiga nya möjligheter.

Upplev fördelarna med SOC 2-rapporter

Under försäljningsprocessen är det vanligt att en kund ber sin leverantör att fylla i ett IT-frågeformulär som har utarbetats av ett team av ingenjörer. En SOC 2-rapport kan nu ge effektiva svar på dessa frågor och snabba upp processen avsevärt. Detta ger också kunden en känsla av förtroende för att processerna verkligen är i ordning.



Presentation Securance

Investera i Effektivitet, Värde och Partnerskap

- **Analysera Risker**
- **Planera Projekt**
- **Förbereda Systembeskrivningar**
- **Genomföra en Beredskapsbedömning**

Att implementera SOC 2 kräver effektiv planering, ledningens engagemang, grundlig analys av processer samt pålitliga resurser och projektledning.

Securance har sitt ursprung i en 'Big Four'-revisionsfirma och grundades 2004. Vår bakgrund innebär att vi arbetar enligt de högsta professionella standarderna och har erfarenhet av att arbeta med snäva tidsramar. Vi lever efter våra professionella standarder och levererar alltid högsta kvalitet, samtidigt som vi kontinuerligt strävar efter att möta våra kunders behov.

Tack vare vår platta struktur och effektiva kommunikationsramverk kan vi snabbt reagera på dina krav. Att välja Securance innebär att välja en professionell organisation, men också en personlig approach. Effektiv projektledning, vår erfarenhet av att implementera riskhanteringsramverk inom din bransch och professionalism är enligt vår mening grunden för utmärkta resultat.

Som Securance tror vi att en god förståelse, tydlig kommunikation och kunskap om våra kunders bransch är avgörande för att leverera mervärde till dig som kund. Baserat på denna strategi kommer vi att hålla dig informerad om relevanta förändringar i lagar, regler och andra viktiga utvecklingar.

SECURANCE
BE SURE

Våra Nöjda Kunder

Referenser

SECURANCE
BE SURE

Securance Ltd.

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

Securance - Seadot

Sidenvävargatan 17
753 19 Uppsala
+46703040656
www.seadot.se

Securance BV

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