SECURANCE

Step-by-step Guide

ISAE 3000 Compliance.

ISAE 3000 Compliance

Outsourcing | Trust Services Criteria

ISAE 3000 is een ISAE-rapport (International Standard on Assurance Engagements) dat zekerheid verschaft over uitbestede processen. Een audit uitgevoerd in overeenstemming met ISAE 3000 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. ISAE 3000-rapporten worden opgesteld in overeenstemming met de Trust Services Criteria.

ISAE 3000 richt zich op de niet-financiële rapportagecontroles van een bedrijf met betrekking tot beveiliging, beschikbaarheid, verwerkingsintegriteit, vertrouwelijkheid en privacy. Deze principes worden uiteengezet in de Trust Services Criteria. Elk van de criteria heeft gedefinieerde vereisten (Points of Focus) die als leidraad dienen om de naleving van de criteria aan te tonen.

Modulair

ISAE 3000-rapporten zijn modulair, wat betekent dat rapporten een of meer van de principes kunnen omvatten, afhankelijk van de behoeften en vereisten van een serviceorganisatie. De enige criteria die verplicht zijn voor ISAE 3000 zijn de beveiligingscriteria. Deze criteria worden ook wel de c criteria genoemd.

Common Criteria

De enige criteria die verplicht zijn voor ISAE 3000 is beveiliging, waarnaar ook wordt verwezen als de Common Criteria, Aanvullende criteria kunnen worden opgenomen binnen de reikwijdte van een ISAE 3000-rapportage.

Naast beveiligingseisen (Logische en fysieke toegangscontroles, Systeemoperaties en Wijzigingsbeheer) bevatten de Gemeenschappelijke Criteria ook eisen voor een raamwerk voor interne controle, inclusief 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 ISAE 3000-rapport door de aandachtspunten en aanvullende criteria te volgen zoals uiteengezet in het COSO-raamwerk 2013 (risicobeheer) en de Trust Services Criteria. Hierna wordt het ISAE 3000-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 ISAE 3000-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.

PHASE 1. DEFINITIE VAN DE SCOPE

Hoe de scope van een ISAE 3000-rapport wordt gedefinieerd

De reikwijdte van een ISAE 3000-rapport heeft betrekking op de (niet-financiële) controles binnen een serviceorganisatie die relevant zijn voor Beveiliging, Beschikbaarheid, Verwerkingsintegriteit, Vertrouwelijkheid en/of Privacy, die zijn gedefinieerd in de Trust Service Criteria. Het ISAE 3000-rapport moet een reikwijdtegedeelte bevatten waarin de belangrijkste onderdelen van de reikwijdte worden vermeld. Het moet details bevatten over de soort(en) diensten die worden geleverd en ook de infrastructuur, software, mensen, beleidsregels en procedures en gegevens die relevant zijn voor deze diensten.

Voorbeeld

Voor een Software as a Service (SaaS)-provider is hun toepassingsgebied meestal hun softwaretoepassing(en) die toegankelijk zijn voor hun klanten. Dit omvat alle gegevens die erin zijn opgeslagen, de infrastructuur die het host en de mensen en procedures die het ondersteunen. De subdienstverleners en aanvullende controlegebieden voor gebruikersentiteiten geven meer details over de reikwijdte in andere secties van het rapport door de grenzen van de reikwijdte binnen het rapport te definiëren.

Conclusie

Uiteindelijk is het aan het management om de reikwijdte van een ISAE 3000-rapport te bepalen. De controles die gericht zijn op de activiteiten van de serviceorganisatie en die substantieel zijn voor de niet-financiële overzichten van de organisatie moeten in de scope worden opgenomen. Naast het feit dat de reikwijdte duidelijk moet worden gedefinieerd en vermeld in het rapport, is er enige flexibiliteit. Uiteindelijk ligt de verantwoordelijkheid om ervoor te zorgen dat het verslag voldoet aan de eisen van de eindgebruikers bij het management.

Concurrentievoordeel

Hoe een ISAE 3000-rapport u een voorsprong geeft op uw concurrenten

ISAE 3000 biedt een concurrentievoordeel door dienstverlenende organisaties te onderscheiden van hun concurrenten. De voordelen van ISAE 3000-rapporten omvatten het verbeteren en afstemmen van risicobeheer, terwijl ook het vertrouwen van de markt wordt bevorderd door een transparante presentatie van het controle framework. De implementatie van ISAE 3000 verbetert de controle-efficiëntie en minimaliseert operationele inefficiënties binnen het bedrijf.

PHASE 2. Implementatie

Stap voor stap aanpak

1. Impact Analyse & Planning

In Fase 1 wordt de impact (GAP-analyse) van de implementatie bepaald en de toepasbaarheid van de Trust Services Criteria beoordeeld. Op basis van de impact en de gedefinieerde 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 de risico's te identificeren, de impact en de bestaande werkwijze te bepalen en kennis te nemen van de aanwezige informatie binnen de organisatie. Op basis van de verkregen informatie uit de interviews worden vervolgens de beheersmaatregelen van de organisatie beschreven aan de hand van de ISAE 3000-eisen. Deze worden vastgelegd in een controlematrix; een matrix met daarin de ISAE 3000 eisen en bijbehorende beheersmaatregelen. Wij adviseren proactief over de implementatie van ontbrekende controls (inclusief procesbeschrijvingen).

3. Control Framework

In fase 3 zal Securance het control framework beschrijven op basis van het meest recente COSO-raamwerk (COSO 2013) en het algemene deel van de rapportage opstellen. In het algemene deel is een beschrijving van de processen, de organisatie en de General IT Controls opgenomen.

4. ISAE 3000 Rapport

In fase 4 wordt het volledige ISAE 3000-rapport opgesteld op basis van de afzonderlijke secties en aanvullende secties zoals de managementverklaring en de aanvullende controles van de gebruikersentiteit. Fase 4 resulteert in een concept ISAE 3000-rapport. Dit rapport wordt in detail

besproken met de betrokken medewerkers. De organisatie zal tijdens deze fase alle geïdentificeerde ontbrekende controles binnen de organisatie implementeren.

De doorlooptijd van de eerste vier fasen zal zes tot acht weken bedragen, afhankelijk van de inzet en beschikbaarheid van werknemers. De vereiste beschikbaarheid van C-level executives is naar verwachting één dag per week gedurende die periode.

5. Pre-Audit

Na het opstellen van het rapport voert Securance in fase 5 een pre-audit of 'walkthrough' uit. Tijdens de pre-audit worden de controlemaatregelen getest en mogelijke probleemgebieden geïdentificeerd voorafgaand aan de definitieve audit. Tijdens deze fase levert de organisatie de documentatie en het bewijsmateriaal dat Securance nodig heeft.

6. Redressing

Tijdens fase 6, als resultaat van de pre-audit, worden verbeteringen in de beheersmaatregelen en het managementsysteem geïmplementeerd en worden oplossingen voorbereid voor de geïdentificeerde probleemgebieden. Securance zal oplossingen aanleveren die geïmplementeerd kunnen worden binnen de organisatie en het ISAE 3000 rapport. Fase 6 zal resulteren in het definitieve ISAE 3000 rapport.

De doorlooptijd van fase 5 en 6 is tussen de twee en vier weken. De vereiste beschikbaarheid van werknemers is naar verwachting één dag per week gedurende die periode.

PHASE 3. De Audit

Quality Assurance Audits

The ISAE 3000 Audits uitgelegd

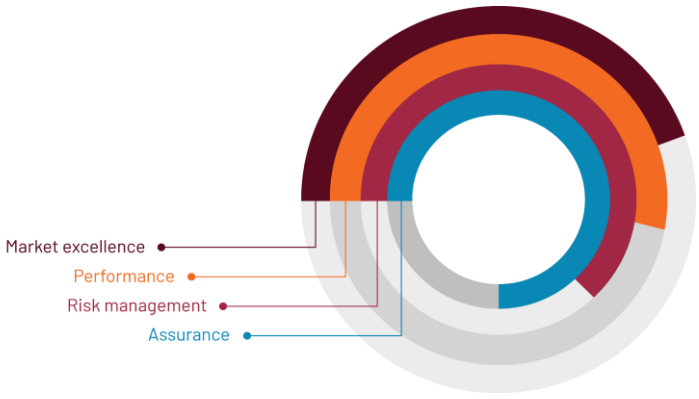
De sleutel tot succesvolle outsourcing is het selecteren van een serviceprovider die uw organisatie begrijpt. Een ISAE 3000-certificering biedt zekerheid over de beveiliging, beschikbaarheid, vertrouwelijkheid, verwerkingsintegriteit en privacy van informatie. Als je te maken hebt met gevoelige klantgegevens, zijn deze elementen belangrijke succesfactoren. In een ISAE 3000-rapport wordt het risicobeheersingsraamwerk beschreven, inclusief de gerelateerde controles en procedures voor het bewaken van het risicobeheersingsraamwerk. Het rapport is opgesteld in overeenstemming met de Trust Services Criteria om een set criteria te bieden voor beveiliging, beschikbaarheid, verwerkingsintegriteit en privacy om gelijke tred te houden met de snelle groei van cloud computing en de uitdagingen op het gebied van bedrijfsuitbesteding die de wereldeconomie biedt.

Type I Report

Een ISAE 3000 Type I-rapport bevat een oordeel van een externe auditor over de controles die op een specifiek moment zijn uitgevoerd. De externe auditor onderzoekt of de controles voldoende zijn ontworpen om een redelijke mate van zekerheid te bieden dat de beweringen in de financiële overzichten worden waargemaakt en of de controles op hun plaats zijn.

Type II Report

In een ISAE 3000 Type II-rapport rapporteert de externe auditor over de geschiktheid van het ontwerp en het bestaan van controles en over de operationele effectiviteit van deze controles in een vooraf gedefinieerde periode van minimaal zes maanden. Dit houdt in dat de externe auditor een gedetailleerd onderzoek uitvoert naar de interne controle van de serviceorganisatie en ook onderzoekt of alle controles effectief werken in overeenstemming met de vooraf gedefinieerde processen en controles.



Belangrijkste voordelen

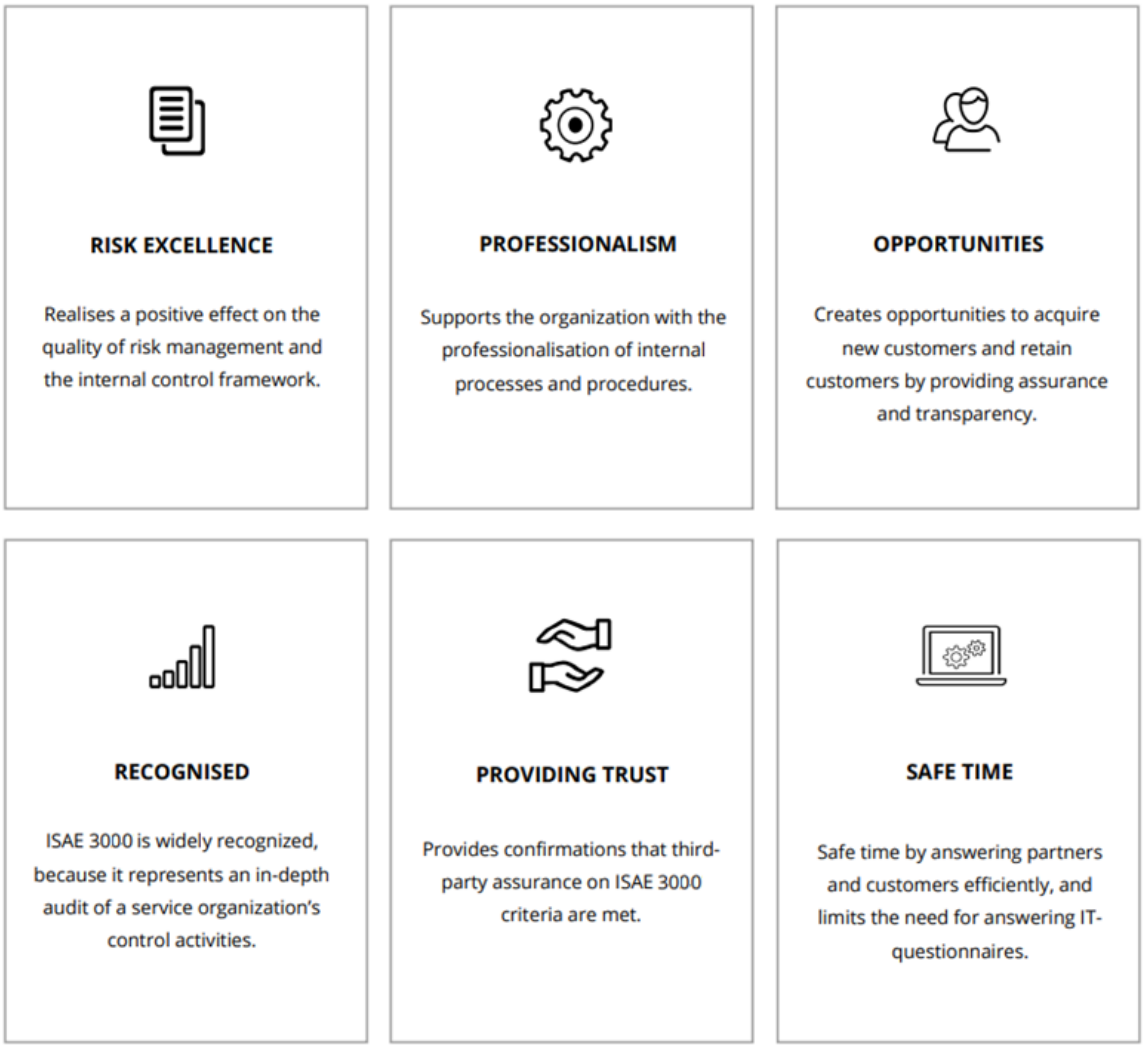
Van ISAE 3000 Compliance

Ervaar de voordelen van ISAE 3000 rapporten

ISAE 3000 rapporten worden door organisaties gebruikt als marketinginstrument. 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 Procurement

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 ingenieurs. Nu zal een ISAE 3000-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.



Maak kennis met Securance

Investeer in efficiëntie, waarde, en partnerschap

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

Het implementeren van ISAE 3000 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