



SECURANCE

Stap-voor-stap Gids
ISAE 3402 Compliance.

Inhoud

Kennismaking met ISAE 3402

In deze whitepaper geven we u de nodige informatie over ISAE 3402. De whitepaper bestaat uit informatie over de ISAE 3402 standaard, de projectfasen van ISAE 3402 compliance (definiëren van de scope, de implementatie en de audit) en de voordelen van ISAE 3402 voor uw organisatie.

Als professioneel Risk Management Governance en Compliance bedrijf bieden wij graag ondersteuning bij het ISAE 3402 compliance project binnen uw organisatie. We beantwoorden graag al uw vragen over ISAE 3402.

ISAE 3402

Uitbesteding | Beveiliging van financiële processen

ISAE 3402 is een internationaal erkende controlestandaard, omdat het een diepgaande controle vertegenwoordigt van de controledoelstellingen en controleactiviteiten van een serviceorganisatie, die vaak controles van informatietechnologie en gerelateerde processen omvatten.

De reikwijdte van het onderzoek van de externe auditor omvat de categorieën transacties in de activiteiten van de serviceorganisatie die van belang zijn voor de financiële overzichten van de gebruikersorganisatie, en processen die specifiek door de serviceorganisatie zijn gedefinieerd. ISAE 3402 is over het algemeen van toepassing wanneer een onafhankelijke auditor ("gebruikende auditor") de controle van financiële overzichten plant van een entiteit ("de gebruikende organisatie") die diensten afneemt van een andere organisatie ("de serviceorganisatie").

Het rapport van de service-auteur, dat het oordeel van de service-auditor bevat, wordt aan de service-organisatie afgegeven bij de afsluiting van een ISAE 3402 assurance-opdracht. ISAE 3402 specificeert geen vooraf bepaalde reeks controledoelstellingen of controleactiviteiten die serviceorganisaties moeten bereiken.

Uitbesteding

Voor uitbestede diensten is informatie van een serviceorganisatie nodig om de risico's van uitbestede diensten aan te pakken. Een ISAE-rapport is een intern controlerapport dat deze informatie verschaft. ISAE 3402 is de standaard voor zekerheid over financiële processen (of processen met een financiële impact voor de gebruikersorganisatie).

De relevante processen, het risicomanagementraamwerk en een gedetailleerde controlematrix moeten door een organisatie worden beschreven. De gedetailleerde controlematrix moet controledoelstellingen en controlebeschrijvingen bevatten.

Na de implementatie moeten alle procedures en controles operationeel zijn. Alle werkprocedures, het beheer van het proces en de discipline van de organisatie moeten uniform zijn om te voldoen aan de beschreven procedures in het rapport.

Industrieën

Organisaties die diensten verlenen aan andere organisaties, bijvoorbeeld Asset/Property Managers, Pension Services Providers, Software As A Service (SaaS)-providers, Infrastructure As A Services (IaaS)-providers, Platform As A Service (PaaS)-providers, en Datacenter Services providers zijn over het algemeen verplicht om een ISAE 3402-rapport te implementeren.

Als uitbestede processen gerelateerd zijn aan financiële processen, is ISAE 3402 relevant. Een ISAE 3000 of SOC 2 kan relevanter zijn als de processen betrekking hebben op General IT Controls (GITC's), beveiliging en/of privacy.

Fase 1. Definitie van de reikwijdte

Hoe bepaal je de reikwijdte van een ISAE 3402-rapport?

De reikwijdte van een ISAE 3402-rapport heeft betrekking op de financiële controles binnen een serviceorganisatie die relevant zijn voor de financiële processen met betrekking tot de geleverde services (of processen met een financiële impact voor de gebruikersorganisatie, als er geen directe financiële transacties worden gedaan).

Het ISAE 3402-rapport moet een reikwijdtegedeelte bevatten waarin de belangrijkste componenten van de reikwijdte worden vermeld, inclusief de inclusie of carve-out van subdienstverleners. Het moet details bevatten over het/de type(n) geleverde diensten, het interne controle framework (gebaseerd op het COSO framework) en een beschrijving van de General IT Controls.

Scope Voorbereiden

De basis voor het opstellen van de scope van het ISAE 3402-rapport zijn de uitbestedingsrisico's (financieel, compliance, operationeel) van de gebruikersorganisatie. Risico's met betrekking tot de ICT-structuur moeten ook binnen deze context worden gedefinieerd. Voor de relevante processen die samenhangen met de geïdentificeerde risico's worden specifieke controledoelstellingen gedefinieerd. Op basis van de opgestelde controledoelstellingen worden controles beschreven om de controledoelstellingen te bereiken en uiteindelijk de uitbestedingsrisico's te beperken. De aanvullende controle van de gebruikersorganisatie geeft verdere details over de reikwijdte, de grenzen van de reikwijdte en de controles die bij de gebruikersorganisatie aanwezig moeten zijn.

Uiteindelijk is het aan het management om de reikwijdte van een ISAE 3402-rapport te definiëren, hoewel het de vereiste is dat de processen die een financieel effect kunnen hebben voor de gebruikersorganisatie ten minste worden opgenomen.

Inclusief of Carve-out?

Als een serviceorganisatie haar processen (deels) uitbesteedt, is er sprake van een zogenaamde subserviceorganisatie. De serviceorganisatie bepaalt of de relevante controles van de subserviceorganisatie zijn beschreven. De ISAE 3402-richtlijnen schrijven hiervoor twee methoden voor; de carve-out methode en de inclusieve methode.

Bij gebruik van de carve-out methode wordt in de beschrijving van de serviceorganisatie expliciet aangegeven dat de controls van de subserviceorganisatie en de bijbehorende controledoelstellingen niet worden meegenomen in de beschrijving van de controls en de scope van de audit door de auditor van de serviceorganisatie. Bij gebruik van de inclusieve methode verklaart de serviceorganisatie dat de beheersingsmaatregelen van de subserviceorganisatie zijn opgenomen in de beschrijving van de beheersingsmaatregelen. Een carve-outmethode kan worden gebruikt als de subserviceorganisatie een ISAE 3402 (SOC 1) of SOC 2-rapport heeft.

Concurrentievoordeel

Hoe een ISAE 3402-Rapport u een voorsprong geeft op uw concurrenten

ISAE 3402 biedt een concurrentievoordeel door serviceorganisaties te onderscheiden van hun concurrenten. De voordelen van ISAE 3402-rapporten variëren van het versterken en verfijnen van risicomanagement tot het winnen van vertrouwen in markten door middel van transparantie van het controle framework.



Fase 2. Implementatie

Stap-voor-stap Aanpak



1. Impactanalyse en reikwijdte

In fase 1 wordt de impact (GAP-analyse) van de implementatie bepaald. Op basis van de impact en de gedefinieerde reikwijdte van de implementatie wordt een gedetailleerd plan opgesteld waarin de verschillende mijlpalen worden geïdentificeerd en afspraken met het management worden gemaakt.

2. Processen en controles

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 volgens de ISAE 3402-eisen. Deze worden vastgelegd in een controlematrix; een matrix met daarin de controledoelstellingen en bijbehorende controls. Wij zullen proactief adviseren over de implementatie van eventueel ontbrekende controls (inclusief procesbeschrijvingen).

3. Control Framework

In fase 3 wordt het raamwerk voor interne controle beschreven op basis van het meest recente COSO-raamwerk (COSO 2013) en het algemene deel als de rapportage is opgesteld. In het algemene gedeelte wordt een beschrijving van de processen, de organisatie en de General IT Controls opgenomen.

4. ISAE 3402 Rapport

In fase 4 wordt het volledige ISAE 3402-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 3402-rapport. We zullen dit rapport in

detail bespreken met het relevante personeel. 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 medewerkers. De vereiste beschikbaarheid van C-medewerkers 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 preaudit of 'doorloop' 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. Verbeteringen

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 3402 rapport. Fase 6 zal resulteren in het definitieve ISAE 3402 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.

Controles Definiëren

Control Types Uitgelegd

Een controle framework bestaat altijd uit General IT Controls, handmatige controles en monitoring controles. Deze controls vormen samen het control framework waarmee risico's worden beheerst. De monitoring controls fungeren als een secundaire 'filter' voor onregelmatigheden die niet zijn gedetecteerd door de primaire management controls. Het interne controle framework bestaat altijd uit een set van controls; controls die samenwerken. Deze set van controls zorgt ervoor dat risico's effectief worden beheerst.

General IT Controls

De General IT Controls zijn de controles die ervoor zorgen dat er voldoende beveiliging en maatregelen voor gegevensintegriteit zijn om te garanderen dat de financiële informatie juist en volledig is ten behoeve van de jaarrekening. Een internationaal erkend raamwerk voor de General IT Controls is het COBIT 5.0 raamwerk.

Applicatie controls

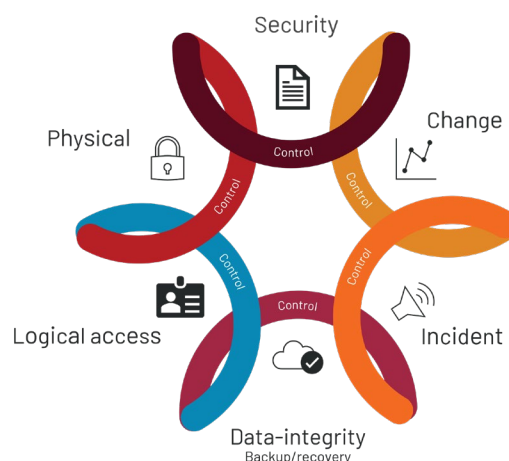
Applicatiecontroles zijn geautomatiseerde controles binnen een systeem of applicatie die worden ingesteld (bijvoorbeeld door middel van een script) om onder andere de volledigheid en integriteit van de invoer en uitvoer van gegevens, autorisatie en authenticatie van gegevens en gebruikers en de beschikbaarheid van systemen te garanderen.

Manual Controls

De handmatige controles zijn de controles die worden uitgevoerd door een bevoegd persoon binnen de gebruikersorganisatie. Dit kan variëren van het testen van software releases tot het autoriseren van financiële transacties in de financiële administratie of het autoriseren van back-up rapporten. De applicatiecontroles ondersteunen de handmatige controles.

Monitoring Controls

De ISAE 3402-richtlijnen schrijven niet expliciet controles op entiteitsniveau of monitoringcontroles voor. Het is echter een goede gewoonte om in het 3402-rapport monitoringcontroles te beschrijven. Idealiter zijn de controles op bedrijfsniveau afgestemd op het COSO-raamwerk. Andere monitoring controls zijn opgenomen binnen de controle matrix per proces.



Fase 3. De Audit

Quality Assurance Audits

De ISAE 3402 Audit

Een ISAE 3402-rapport stelt serviceorganisaties in staat om hun controleactiviteiten en -processen in een uniforme rapportagevorm bekend te maken aan hun klanten en de auditors van hun klanten. Het service-auditorrapport, dat het oordeel van de service-auditor bevat, wordt aan het einde van de audit aan de serviceorganisatie verstrekt.

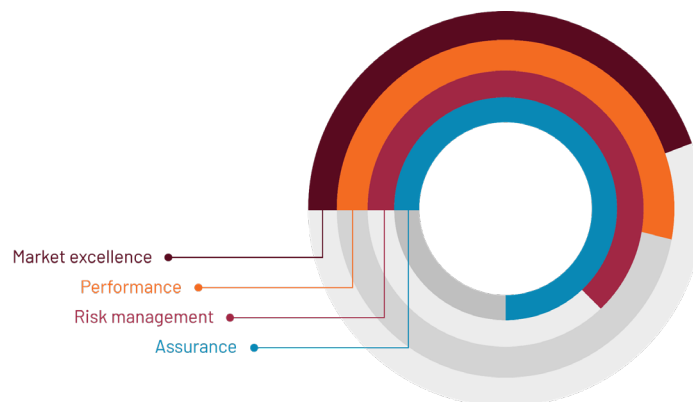
ISAE 3402 specificeert geen vooraf bepaalde reeks controledoelstellingen of controleactiviteiten die serviceorganisaties moeten bereiken. Het identificeren en evalueren van relevante controles is over het algemeen een belangrijke stap in de algehele aanpak van de gebruiker-auditor voor de controle van financiële overzichten. Een service-auditor kan twee soorten rapporten afgeven; een Type I-rapport of een Type II-rapport.

Type I Rapport

Een ISAE 3402 Type I-rapport bevat een oordeel van een externe auditor over de controles die op een specifiek moment in werking zijn getreden. 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 Rapport

In een ISAE 3402 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 3402 Compliance

Ervaar de voordelen van ISAE 3402-rapporten

ISAE 3402-rapporten worden door organisaties gebruikt als marketinginstrument. Nieuwe en bestaande klanten herkennen direct dat ze te maken hebben met een betrouwbare partij. Organisaties die niet over een dergelijke rapportage beschikken, lopen mogelijk belangrijke nieuwe kansen mis. Tijdens het verkoopproces is het gebruikelijk dat een klant zijn leverancier vraagt om een vragenlijst in te vullen om inzicht te krijgen in het huidige volwassenheidsniveau van de organisatie. Nu zal een ISAE 3402-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 op orde zijn.



RISK EXCELLENCE

Realises a positive effect on the quality of risk management and the internal control framework.



PROFESSIONALISM

Supports the organization with the professionalisation of internal processes and procedures.



OPPORTUNITIES

Creates opportunities to acquire new customers and retain customers by providing assurance and transparency.



RECOGNISED

ISAE 3402 is widely recognized, because it represents an in-depth audit of a service organization's control activities.



PROVIDING TRUST

Provides confirmations that third-party assurance on ISAE 3402 criteria are met.



SAFE TIME

Safe time by answering partners and customers efficiently, and limits the need for answering IT-questionnaires.

Wij zijn Securance

Investeer in efficiëntie, waarde en partnerschap

- Risico's analyseren
- Het project plannen
- Systeembeschrijvingen voorbereiden
- Een Readiness Assessment uitvoeren

Het implementeren van ISAE 3402 vereist effectieve planning, betrokkenheid van de leiding, grondige analyse van processen en betrouwbare middelen en projectmanagement.

Securance komt voort uit een 'Big Four' accountantskantoor en is opgericht in 2004. Het resultaat van onze achtergrond is dat we werken volgens de hoogste professionele standaarden en ervaring hebben in het werken met strakke deadlines. We leven naar onze professionele normen en leveren altijd de hoogste kwaliteit, terwijl we er voortdurend naar streven om aan de behoeften van onze klanten te voldoen.

Door onze vlakke structuur en efficiënte communicatie kunnen we snel reageren op uw behoeften. Kiezen voor Securance betekent kiezen voor een professionele organisatie, maar ook kiezen voor een persoonlijke benadering. Effectief projectmanagement, onze ervaring met het implementeren van risicomanagementtraamwerken in uw branche en professionaliteit zijn volgens ons de basis voor uitstekende resultaten.

Als Securance geloven wij dat een goed begrip, heldere communicatie en kennis van de branche van onze klanten essentieel zijn voor het leveren van toegevoegde waarde aan u als klant. Op basis van deze benadering informeren wij u over de relevante veranderingen in wet- en regelgeving en andere belangrijke ontwikkelingen.



Onze Tevreden Klanten

Referenties





Securance Ltd.

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

Securance BV

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