ISAE 3402 Compliance.

Stappenplan - ISAE 3402

ISAE3402.nl

Introductie

Maak Kennis Met ISAE 3402

In dit stappenplan zullen we u voorzien van de noodzakelijke informatie over ISAE 3402. De whitepaper bestaat uit informatie met betrekking tot de ISAE 3402 standaard, de projectfasen van ISAE 3402 naleving (het definiëren van de scope, de implementatie en de audit), en de voordelen van ISAE 3402 voor uw organisatie.

Als een professioneel bedrijf op het gebied van Risicobeheer, Bestuur en Naleving, zijn we verheugd om ondersteuning te bieden bij het ISAE 3402 nalevingsproject binnen uw organisatie. Onze uitgebreide aanpak zorgt ervoor dat we samen met u alle vereisten volledig in kaart brengen en implementeren. Dit omvat het analyseren van risico's, het opstellen van een robuust controlekader, en het begeleiden van uw organisatie door elke stap van het proces.

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 risicobeheer tot het verkrijgen van vertrouwen op markten door middel van transparantie van het beheerskader.

We staan meer dan graag klaar om eventuele vragen te beantwoorden die u mogelijk heeft met betrekking tot ISAE 3402.

ISAE 3402

Beveiliging en controle van financiële processen

ISAE 3402 is een internationaal erkende standaard die een diepgaande beoordeling biedt van de controle-objectieven en -activiteiten van dienstverlenende organisaties. Het wordt vaak toegepast op informatietechnologie en aanverwante processen, en is essentieel voor organisaties die financiële gegevens verwerken namens hun klanten.

De externe auditor onderzoekt processen die van invloed zijn op de financiële overzichten van gebruikersorganisaties. Dit omvat transacties en activiteiten die specifiek door de dienstverlener worden gedefinieerd. ISAE 3402 wordt vooral relevant wanneer een gebruikersauditor de financiële overzichten van een organisatie beoordeelt die afhankelijk is van een externe dienstverlener.

Bij afronding van de opdracht verstrekt de auditor een rapport aan de dienstverlener. Dit rapport biedt transparantie en stelt gebruikersorganisaties in staat om beter inzicht te krijgen in de risicobeheersing bij de dienstverlener. Anders dan sommige andere standaarden specificeert ISAE 3402 geen vaste set controle-objectieven of -activiteiten. Elke dienstverlener definieert deze op basis van de specifieke behoeften van zijn klanten.

Uitbesteding en risicobeheersing

Uitbestede diensten brengen unieke risico's met zich mee, waardoor een duidelijk overzicht van interne controles vereist is. Een ISAE 3402-rapport biedt zekerheid over de betrouwbaarheid van financiële processen en andere bedrijfsactiviteiten die een financiële impact hebben op de gebruikersorganisatie.

Om een ISAE 3402-rapport te realiseren, moeten dienstverleners:

- Relevante processen en risico's identificeren.
- Een gedetailleerd beheerskader ontwikkelen.
- Regelmatige monitoring en evaluatie uitvoeren om consistentie en naleving te waarborgen.

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

Relevante industrieën

ISAE 3402 wordt breed toegepast door organisaties die essentiële diensten leveren aan andere bedrijven, zoals:

- Vermogens- en vastgoedbeheerders
- Pensioendienstverleners
- Software-as-a-Service (SaaS)-aanbieders
- Infrastructure-as-a-Service (IaaS)- en Platform-as-a-Service (PaaS)-aanbieders
- Datacenterdienstverleners

Wanneer de uitbestede processen primair betrekking hebben op financiële processen, is ISAE 3402 de aangewezen standaard. Voor processen die gericht zijn op IT-beheersmaatregelen, beveiliging of privacy, kan een ISAE 3000- of SOC 2-rapport geschikter zijn. Het maken van de juiste keuze hangt af van de aard van de diensten en de specifieke vereisten van de gebruikersorganisatie.

Met een zorgvuldig uitgevoerd ISAE 3402-traject kunnen dienstverlenende organisaties zowel hun risicobeheersing verbeteren als het vertrouwen van hun klanten versterken.

Fase 1. Definitie van de Scope

Het bepalen van de scope van een ISAE-3402 rapport

Het definiëren van de scope van een ISAE 3402-rapport begint met een duidelijke vraag: welke processen en diensten binnen uw organisatie hebben een directe financiële impact op de gebruikersorganisatie? Dit is geen eenvoudige checklist, maar een proces dat zorgvuldige overweging vereist.

Eerst is het belangrijk om alle relevante diensten in kaart te brengen. Denk hierbij aan de specifieke activiteiten die uw organisatie uitvoert en bepaal of en hoe uitbesteed personeel betrokken is bij deze processen. Het is van cruciaal belang om de aard van deze diensten te begrijpen en te documenteren, samen met een overzicht van de betrokken processen en een beschrijving van het interne beheerskader. Dit beheerskader, gebaseerd op het COSO-framework, vormt de basis voor een goed gestructureerd rapport.

Bij het in kaart brengen van de scope moet u ook de risico's identificeren. Uitbestedingsrisico's – zoals financiële, nalevings- en operationele risico's – moeten grondig worden geanalyseerd. Ook risico's binnen de ICT-structuur mogen niet worden vergeten, aangezien deze vaak een directe invloed hebben op de kwaliteit en betrouwbaarheid van de processen. Zodra deze risico's duidelijk zijn, kunt u beginnen met het opstellen van controleobjectieven. Deze objectieven dienen als richtlijn voor de beheersmaatregelen die nodig zijn om risico's te beheersen en de gestelde doelen te behalen.
De volgende stap is het ontwerpen van deze beheersmaatregelen. Het is belangrijk om gedetailleerd te beschrijven hoe elke maatregel helpt om specifieke risico's te mitigeren. Hier hoort ook een overzicht bij van de Algemene IT-Beheersmaatregelen die bijdragen aan een solide interne controle.

Aanvullende controles binnen de gebruikersorganisatie kunnen ook worden opgenomen. Deze bieden meer inzicht in de grenzen van de scope en zorgen ervoor dat er geen lacunes in het risicobeheer zijn. Het is tenslotte aan het management om de definitieve scope vast te stellen. Hierbij is het essentieel dat alle processen met een significante financiële impact worden opgenomen.

Een laatste overweging bij het definiëren van de scope is hoe om te gaan met uitbestede processen die door subdienstverleners worden uitgevoerd. Hier biedt ISAE 3402 twee opties: de inclusieve methode, waarbij de beheersmaatregelen van de subdienstverlener worden opgenomen, en de uitsluitingsmethode, waarbij deze expliciet worden uitgesloten als de subdienstverlener over een eigen ISAE 3402-rapport beschikt.

Het definiëren van de scope is meer dan een technische oefening; het is een strategische stap die bepaalt hoe uw organisatie risico's beheert en vertrouwen opbouwt bij gebruikersorganisaties. Door dit proces zorgvuldig uit te voeren, legt u een solide basis voor een succesvol ISAE 3402-rapport.

Inclusief of Carve-out?

Wanneer een dienstverlenende organisatie (gedeeltelijk) haar processen uitbesteedt, wordt dit een zogenaamde subdienstverlenende organisatie genoemd. De dienstverlenende organisatie moet bepalen of de relevante beheersmaatregelen van de subdienstverlenende organisatie worden opgenomen in het ISAE 3402-rapport. Deze keuze is cruciaal omdat het de reikwijdte en het detailniveau van het rapport bepaalt.

De ISAE 3402-richtlijnen bieden twee benaderingen:

1. **Uitsluitingsmethode:**
    - Bij deze methode vermeldt de beschrijving van de dienstverlenende organisatie expliciet dat de beheersmaatregelen van de subdienstverlenende organisatie en de bijbehorende beheersdoelstellingen niet zijn opgenomen in het rapport. Dit geldt ook voor de controles en de reikwijdte van de audit door de auditor van de dienstverlenende organisatie. De verantwoordelijkheid voor de beheersmaatregelen ligt dan volledig bij de subdienstverlener, op voorwaarde dat deze een eigen ISAE 3402 (SOC 1) of SOC 2-rapport heeft.

2. **Inclusieve methode:**
    - Bij deze methode worden de beheersmaatregelen van de subdienstverlenende organisatie opgenomen in het rapport. De dienstverlenende organisatie verklaart in dit geval expliciet dat deze maatregelen deel uitmaken van de beschrijving van de beheersmaatregelen. Dit vereist nauwe samenwerking met de subdienstverlener om ervoor te zorgen dat alle relevante controles correct worden beschreven en beoordeeld.

De keuze tussen de inclusieve en uitsluitingsmethode hangt af van de invloed van subdienstverleners op uitbestede processen en de beschikbaarheid van hun eigen rapportage. Bij meerdere subdienstverleners kan een hybride aanpak worden toegepast. Beide methoden vereisen duidelijke documentatie en communicatie om een balans te vinden tussen transparantie, controle en haalbaarheid bij het opstellen van het ISAE 3402-rapport.

FASE 2. Implementatie

Stapsgewijze Aanpak

1. Impact Analyse & Planning

In Fase 1 wordt de impact (GAP-analyse) van de implementatie bepaald. 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. Dit plan dient als blauwdruk voor de verdere uitvoering.

2. Processen & Beheersmaatregelen

In Fase 2 worden interviews gehouden om risico's te identificeren, de impact en de bestaande werkwijze te bepalen, en aantekeningen te maken van de aanwezige informatie binnen de organisatie. Vervolgens worden de beheersmaatregelen van de organisatie beschreven volgens de ISAE 3402-vereisten op basis van de informatie verkregen uit de interviews. Deze maatregelen worden gestructureerd in een beheersmatrix, die controle-objectieven en bijbehorende maatregelen koppelt. We zullen proactief advies geven over de implementatie van ontbrekende beheersmaatregelen (inclusief procesbeschrijvingen).

3. Control Framework

In Fase 3 wordt het interne beheerskader beschreven op basis van het meest recente COSO-kader (COSO 2013) en het algemene gedeelte als het rapport wordt voorbereid. In het algemene gedeelte wordt een beschrijving opgenomen van de processen, de organisatie en de Algemene IT-Beheersmaatregelen.

4. ISAE 3402 Rapport

In Fase 4 wordt het volledige ISAE 3402-rapport voorbereid op basis van de individuele secties en aanvullende secties zoals de managementverklaring en de aanvullende gebruikersentiteit controles. Fase 4 resulteert in een concept ISAE 3402-rapport. Het rapport wordt besproken met relevante medewerkers en aangepast waar nodig. De organisatie zal tijdens deze fase eventuele geïdentificeerde ontbrekende beheersmaatregelen implementeren binnen de organisatie.

De verwerkingstijd van de eerste vier fasen zal tussen de zes tot acht weken zijn, afhankelijk van de betrokkenheid en beschikbaarheid van medewerkers. De verwachte beschikbaarheid van medewerkers van categorie C is één dag per week gedurende die periode.

5. Pre-Audit

Na de voorbereiding van het rapport moet een pre-audit of 'walkthrough' uit worden gevoerd. Tijdens de pre-audit worden de beheersmaatregelen getest en mogelijke probleemgebieden geïdentificeerd voordat de definitieve audit plaatsvindt. De organisatie verstrekt benodigde documentatie en bewijsstukken aan de auditor. Deze stap zorgt ervoor dat de organisatie goed is voorbereid op de definitieve audit.

6. Verbeteringen Doorvoeren

Tijdens Fase 6 worden als gevolg van de pre-audit verbeteringen in de beheersmaatregelen en het managementsysteem doorgevoerd en worden oplossingen voor de geïdentificeerde probleemgebieden voorbereid. Eventuele lacunes worden aangepakt, en oplossingen worden geïmplementeerd in lijn met de ISAE 3402-eisen. Deze fase resulteert in het definitieve ISAE 3402-rapport.

De verwerkingstijd van punt 5 en 6 bedraagt tussen de twee en vier weken. De verwachte beschikbaarheid van medewerkers is één dag per week gedurende die periode.

Beheersmaatregelen Definiëren

Soorten Beheersmaatregelen

Een beheerskader bestaat altijd uit Algemene IT-Beheersmaatregelen, handmatige beheersmaatregelen en bewakingsbeheersmaatregelen. Deze beheersmaatregelen vormen samen het beheerskader waarmee risico's worden beheerd. Bewakingsmaatregelen dienen als een extra 'veiligheidsnet' om afwijkingen te detecteren die niet door primaire maatregelen worden opgevangen. Het interne beheerskader bestaat altijd uit meerdere soorten maatregelen die samenwerken om een robuust controlesysteem te bieden

Algemene IT Beheersmaatregelen

De algemene IT-beheersmaatregelen zijn de maatregelen die ervoor zorgen dat er voldoende beveiligings- en gegevensintegriteitsmaatregelen zijn genomen om ervoor te zorgen dat financiële informatie nauwkeurig en volledig is voor het opstellen van de financiële overzichten. Het COBIT 2019-kader wordt nu veelal als referentie gebruikt voor deze maatregelen vanwege zijn bredere focus op IT-governance.

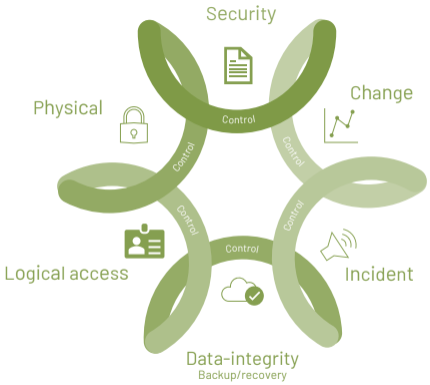
Toepassingsbeheersmaatregelen

Toepassingsbeheersmaatregelen zijn geautomatiseerde controles binnen een systeem of toepassing die zijn ingesteld (bijvoorbeeld door middel van een script) en die onder andere de volledigheid en integriteit van de invoer en uitvoer van gegevens, autorisatie en authenticatie van gegevens en gebruikers, en beschikbaarheid van systemen kunnen waarborgen.

Handmatige Beheersmaatregelen

Handmatige beheersmaatregelen worden uitgevoerd door een geautoriseerd persoon binnen de organisatie. Voorbeelden hiervan zijn het testen van software-updates, het goedkeuren van financiële transacties en het verifiëren van back-uprapporten. Hoewel deze maatregelen meer tijd en inspanning vereisen, spelen ze een cruciale rol bij het waarborgen van compliance en het beperken van risico's.

.



Monitor Maatregelen

De ISAE 3402-richtlijnen vereisen geen expliciete organisatiebrede bewakingsmaatregelen, maar het is een goede praktijk om deze op te nemen in het rapport. Deze maatregelen zijn vooral nuttig voor het tijdig detecteren van afwijkingen en het verbeteren van het risicobeheer. Bij voorkeur worden de bewakingsmaatregelen afgestemd op het COSO-kader en opgenomen in de beheersmatrix per proces. Dit verhoogt de consistentie en transparantie binnen de organisatie.

FASE 3. De Audit

Kwaliteitsborgings Audits

De ISAE 3402 Audit

Een ISAE 3402-rapport stelt dienstverlenende organisaties in staat om hun beheersactiviteiten en processen aan hun klanten en de auditors van hun klanten te openbaren in een uniform rapportageformaat. Het rapport van de dienstauditor, inclusief de mening van de dienstauditor, wordt aan het einde van de audit aan de dienstverlenende organisatie verstrekt.

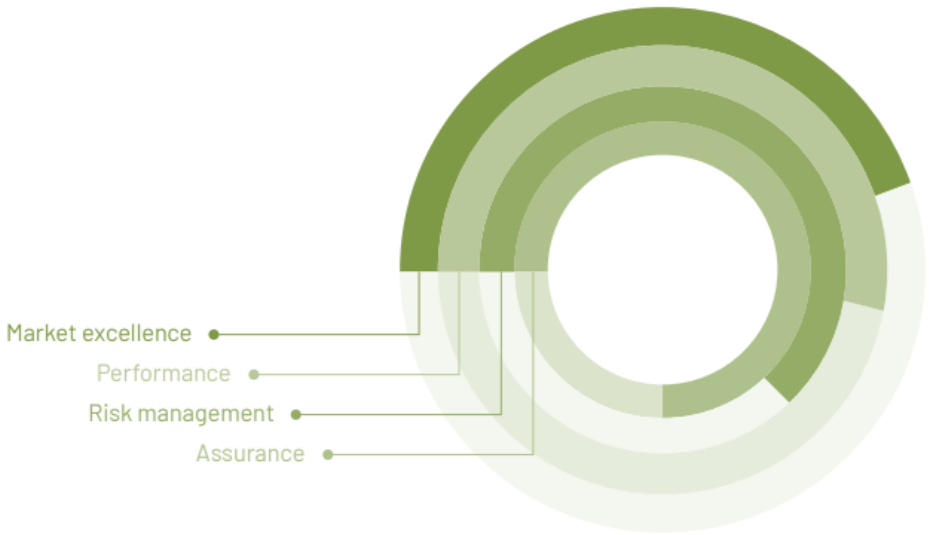
ISAE 3402 specificeert geen vooraf bepaalde set controle-doelstellingen of controle-activiteiten die dienstverlenende organisaties moeten bereiken. Het identificeren en evalueren van relevante controles is over het algemeen een belangrijke stap in de algehele aanpak van de gebruikersauditor voor de controle van financiële overzichten. Een dienstauditor kan twee soorten rapporten uitgeven; een Type I-rapport of een Type II-rapport.

Type I Rapport

Een ISAE 3402 Type I-rapport omvat een mening van een externe auditor over de beheersmaatregelen die op een specifiek moment in de tijd zijn geïmplementeerd. De externe auditor onderzoekt of de beheersmaatregelen adequaat zijn ontworpen om een redelijke zekerheid te bieden dat de financiële overzichtsbeweringen worden bereikt en of de beheersmaatregelen aanwezig zijn.

Type II Rapport

In een ISAE 3402 Type II-rapport rapporteert de externe auditor over de geschiktheid van het ontwerp en de aanwezigheid van beheersmaatregelen, evenals over de operationele effectiviteit van deze beheersmaatregelen in een vooraf bepaalde periode van ten minste zes maanden. Dit houdt in dat de externe auditor een gedetailleerd onderzoek uitvoert naar de interne controle van de dienstverlenende organisatie en ook onderzoekt of alle beheersmaatregelen effectief werken in overeenstemming met de vooraf bepaalde processen en controles.



Voordelen

Van ISAE 3402 Naleving

Ervaar de Voordelen van ISAE 3402-rapporten

ISAE 3402-rapporten worden door organisaties gebruikt als een marketinginstrument. Nieuwe en bestaande klanten herkennen direct dat ze te maken hebben met een betrouwbare partij. Organisaties die niet over dergelijke rapportage beschikken, missen mogelijk belangrijke nieuwe kansen. Tijdens het verkoopproces is het gebruikelijk dat een klant aan hun 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 bieden. Dit zal het proces aanzienlijk versnellen. Dit geeft de klant ook het gevoel en het vertrouwen dat processen daadwerkelijk op orde zijn.

	**RISICO EXCELLENTIE**	Realiseert een positief effect op de kwaliteit van risicobeheer en het interne controlekader.
	**PROFESSIONALITEIT**	Ondersteunt de organisatie bij de professionalisering van interne processen en procedures.
	**KANSEN**	Creëert mogelijkheden om nieuwe klanten aan te trekken en bestaande klanten te behouden door zekerheid en transparantie te bieden.
	**HERKENNING**	ISAE 3402 is breed erkend omdat het een diepgaande audit van de controleactiviteiten van een dienstverlenende organisatie vertegenwoordigt.
	**VERTROUWEN BIEDEN**	Biedt bevestigingen dat derden zekerheid hebben over de naleving van ISAE 3402-criteria.
	**TIJD BESPAREN**	Bespaart tijd door partners en klanten efficiënt te beantwoorden en de behoefte aan het beantwoorden van IT-vragenlijsten te verminderen.