CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

STAPPENPLAN ISAE 3402

Stap voor stap naar een ISAE 3402 verklaring

ISAE 3402 staat voor International Standard for Assurance Engagements. Het is een audit standaard voor rapportage over beheersing van processen die zijn uitbesteed. Een ISAE-verklaring is gericht op organisaties die in aanmerking komen voor een onderzoek naar de geïmplementeerde beheersmaatregelen om de kritische processen van een klant te beveiligen. Wil je een ISAE 3402 verklaring behalen? Dan is het zaak om onderstaande hoofdstappen te doorlopen.

Stap 1: Over de organisatie

In stap 1 wordt er gekeken naar de context van de organisatie met daarin de visie en missie. Het is hierbij van belang dat er wordt gekeken naar de rechtsvorm van de organisatie. Valt de organisatie onder een holding, is het een besloten vennootschap, of betreft het bijvoorbeeld een zzp'er?

Stap 2: Vaststellen van de scope

In deze stap dient de scope, waarvoor de ISAE 3402 verklaring af wordt gegeven, vastgesteld te worden. Denk daarbij aan de scope van een proces, van een applicatie en/of van een aantal beheersmaatregelen.

Stap 3: Uitvoeren van een risicoanalyse

Vervolgens wordt er gekeken naar de risicomanagementfilosofie van de directie/organisatie. Denk daarbij aan degene(n) die verantwoordelijk is/zijn voor het mitigeren van de risico's en degene(n) die dit audit(en). In navolging daarvan wordt er gekeken naar de risicobereidheid van de organisatie, met daaraan gekoppeld de vraag 'wat kan de klant overkomen als het mis gaat'? De risico's die binnen de scope vallen kunnen onderverdeeld worden in verschillende typen, namelijk:

- Risico's t.g.v. technische oorzaken
- Risico's t.g.v. personele oorzaken
- Risico's t.g.v. applicatie-oorzaken
- Risico's m.b.t. de beveiliging
- Risico's m.b.t. integriteit
- Risico's m.b.t. reputatie

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Dit alles wordt weergegeven in een risicoanalyse, met daaraan gekoppeld een waarde die wordt uitgedrukt door de kans maal het effect. Op basis van deze classificatie bepaalt de organisatie haar risicobereidheid.

Stap 4: Integriteit en ethische waarden

De directie en het management van de organisatie hebben een breed scala aan (sociale) beheersmaatregelen getroffen die bijdragen aan de vorming en instandhouding van de door de organisatie gewenste organisatiecultuur. Tijdens deze stap zal er worden gekeken naar de gedragscode en bedrijfswaarden. Deze hebben namelijk invloed op het opstellen van de doelstellingen en de wijze waarop deze doelstellingen moeten worden verwezenlijkt.

Stap 5: Opstellen doelstellingen van de onderneming

In deze stap wordt gekeken naar de doelen die zijn gesteld voor de komende periode om ervoor te zorgen dat de organisatie in control is. Tevens wordt daarbij bekeken of de organisatie voldoet aan haar eigen eisen.

Stap 6: Maatregelen

Naar aanleiding van het vaststellen van de risico's met de daarbij behorende doelstellingen, wordt er gekeken naar de verschillende beheersmaatregelen die geïmplementeerd moeten worden om de risico's te beheersen.

Stap 7: Monitoren en meten van de maatregelen op de effectiviteit

In deze stap wordt concreet gemaakt op welke wijze de beheersmaatregelen, die in voorgaande stap zijn beschreven, worden gemonitord en gemeten. Het is hierbij belangrijk om de beheersmaatregelen te koppelen aan de doelstellingen die zijn vastgesteld. Wellicht is het ook verstandig om de maatregel te koppelen aan het risico om een beter beeld te krijgen van de correlatie.

De controleactiviteiten zijn belangrijk om aan te tonen op welke wijze de getroffen maatregelen werken of niet werken. Er komt dus een overzicht van de doelstelling, de getroffen maatregel en de daarbij uitgevoerde werkzaamheden. De uitkomsten hiervan kunnen bijvoorbeeld worden besproken tijdens een kwartaalmeeting.

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

STAPPENPLAN ISAE 3402

Stap 8: Beheersactiviteiten

De controleactiviteiten vormen een belangrijk onderdeel van de maatregelen die getroffen zijn voor de interne beheersing. Hier dient een agenda voor opgesteld te worden met daarin een minimaal aantal onderwerpen die aan bod moeten komen. Dit alles wordt ook gerapporteerd naar de klant. De onderwerpen zijn:

- Een terugblik op het afgelopen kwartaal;
- Een vooruitblik op komend kwartaal;
- Strategische zaken.

Stap 9: Wijzigingen

Wijzigingen binnen de organisatie kunnen van invloed zijn op de geïmplementeerde risico's en beheersmaatregelen. Het is daarom belangrijk om veranderingen conform een vast proces te laten verlopen in de vorm van indienen, accepteren, beoordelen, goedkeuren, implementeren en evalueren. Het zogenaamde 'change proces' is gebaseerd op ITIL en in lijn met gerelateerde processen die binnen de scope van de verklaring vallen.

Advies en ondersteuning bij ISAE 3402

Bij CertificeringsAdvies Nederland willen we mensen & organisaties inspireren om de toegevoegde waarde van (bedrijfs)normen en wet- en regelgeving op een praktische wijze te implementeren door het aanbieden van advies-, trainings- en outsourcingsdiensten.

Wil je een ISAE 3402 verklaring behalen, maar heb je vragen of ben je benieuwd naar de mogelijkheden met betrekking tot de implementatie? Neem dan gerust eens contact met ons op. Onze gespecialiseerde adviseur helpt je graag op weg.

Meer weten over de mogelijkheden met betrekking tot ISAE 3402?
Neem gerust contact met ons op. Wij helpen je graag.

CertificeringsAdvies Nederland | T: 085-4879972 | E: info@certificeringsadvies.nl