ISAE 3402: Aantoonbare IT assurance

De ISAE 3402 is een IT assurance rapport waarmee organisaties aantoonbaar kunnen maken dat ze in control zijn over hun IT en dat processen op de juiste manier zijn ingericht en worden uitgevoerd. Kiwa heeft jarenlange ervaring op het gebied van informatiebeveiliging en certificering hiervan in diverse sectoren.

Als dienstverlenende organisatie kunt u vandaag de dag niet zonder erkenning door middel van externe certificering. Klanten verlangen aantoonbare kwaliteit. Naast ISO en SAS70 wordt ook ISAE 3402 steeds vaker gevraagd. Het is een van de weinige certificeringen waarbij maatregelen van kwaliteit ook daadwerkelijk op werking worden getoetst. Het management van de organisatie moet ook nog eens schriftelijk verklaren dat het stelsel functioneert. Het zijn internationaal erkende certificeringen en bruikbaar over de hele wereld.
De ISAE 3402 is geschikt voor organisaties die actief in de dienstverlening of organisaties die delen van hun bedrijfskritieke proces hebben uitbesteed en hierover een garantie willen hebben dat dit op de juiste manier is gebeurd. Denk hierbij aan vragen: hoe gaat mijn leverancier om met wet- en regelgeving op het gebied van privacy zoals de AVG ?, of is er wel een goed wijzigingsproces?

ISAE 3402 Type 1 en Type 2

Bij een ISAE 3402 beoordeelt een onafhankelijke (RE-)auditor de kwaliteit van de uitbestede activiteiten van een serviceorganisatie aan de gebruikersorganisatie en het daardoor ‘in-control’ zijn over deze activiteiten door de gebruikersorganisatie. De ISAE 3402 verklaring kan afgegeven worden in een Type 1 en Type 2 verklaring/ rapportage.
ISAE 3402 Type 1 Opzet en bestaan
Doordat een ISAE 3402 type 1 rapport betrekking heeft op één specifieke datum, is een type 1 rapportage voor een gebruikersorganisatie en haar accountant beperkt bruikbaar omdat hieruit niet blijkt of maatregelen ook goed gewerkt hebben gedurende een bepaalde periode. Een ander verschil tussen een type 1 en een type 2 rapportage is dat de auditor zijn bevindingen niet verplicht hoeft op te nemen in de rapportage.

Expert Center Cybersecurity
Kiwa Nederland
cybersecurity@kiwa.com
+31 (0)88 998 49 00

ISAE 3402 Type 2 Opzet, bestaan en werking

Een ISAE 3402 type 2 is inhoudelijk hetzelfde rapport als een type 2 rapport. Hierbij is alleen in de verklaring van de RE auditor nog opgenomen dat de beschreven beheersmaatregelen over een periode van minimaal zes maanden effectief gewerkt hebben. Een gevolg hiervan is dat de controle veel uitgebreider is dan een type 2 audit. Zo worden beheersmaatregelen die iedere dag worden uitgevoerd tussen de 15 tot 25 per jaar getoetst op hun effectieve werking.

Een gebruikersorganisatie heeft met een type 2 rapportage meer zekerheid dat de dienstverlening beheerst wordt zoals is overeengekomen. De periode waarin de ISAE type 2 audit plaatsvindt, is minimaal zes maanden, tenzij er een bijzondere situatie is, zoals de aankoop van een nieuw organisatie onderdeel of een nieuw IT-systeem.

ISAE 3402 audit

De ISAE 3402 audit ziet er op hoofdlijnen als volgt uit. Allereerst wordt de scope bepaald. Hierbij wordt gekeken naar de organisatie, haar beleid en processen en de maatregelen die geïmplementeerd zijn en het beoogde doel wat getracht wordt te bereiken. Op basis hiervan wordt een GAP-analyse uitgevoerd. Zo wordt bepaalt waar u staat, waardoor u eventuele tekortkomingen nog in orde kunt maken.

Hierna vindt de daadwerkelijke toetsing plaats waarbij de maatregelen getest en gevalideerd worden. Er wordt hierbij o.a. gekeken naar de effectiviteit, de relatie tot de geïdentificeerde risico's en hoe het proces beheerst wordt. Over de bevindingen wordt vervolgens gerapporteerd en dit wordt met u inhoudelijk besproken. Omdat ISAE 3402 zich richt op de achterliggende periode zal deze audit op jaarlijkse basis plaatsvinden.

Verplichte aspecten ISAE-rapportage

- Een beschrijving van het interne controle raamwerk;
- Een bevestiging van de serviceorganisatie;
- Een service auditor assurance rapport.

Er zijn dus wel verplichte onderdelen voorgeschreven, maar niet voor alle onderdelen is opgenomen op welke wijze deze onderdelen gepresenteerd moeten worden in de rapportage.

Waarom een ISAE 3402 audit door Kiwa?

Kiwa heeft jarenlange ervaring op het gebied van informatiebeveiliging en certificering hiervan in diverse sectoren. Een ISAE 3402 assurance rapport kan bijdragen een aan verdere diepgang in de aantoonbaarheid van de beheersing van de IT Processen aan klanten en andere stakeholders.

Kiwa kan hierbij helpen door middel van het uitvoeren van:

- Workshop – gezamenlijk vaststellen wat de scope van het onderzoek wordt;
- Tussentijdse GAP-analyses – weten waar u staat;
- Type I assurance rapport – Opzet en bestaan van uw maatregelen;
- Type II assurance rapport – Opzet, bestaan en werking van uw maatregelen;
- De ISAE 3402 certificering gecombineerd uit te voeren met de ISO 27001. Hierbij wordt er een auditmoment gecreerd en dezelfde auditoren ingezet voor beide audits.

Expert Center Cybersecurity
Kiwa Nederland
cybersecurity@kiwa.com
+31 (0)88 998 49 00

Wilt u meer weten over de ISAE 3402 of hoe u deze norm kunt integreren met uw bestaande ISO 27001 certificering? Neem dan vrijblijvend contact met ons op.

Expert Center Cybersecurity
Kiwa Nederland
cybersecurity@kiwa.com
+31 (0)88 998 49 00