DUIJNBORGH AUDIT®

ISAE 3402 verklaring type 1 en 2

Voor klanten van serviceorganisaties draait het om Vertrouwen met een grote V.
Klanten willen blindelings kunnen vertrouwen op de dienstverlening van serviceorganisaties. Het is aan het management van serviceorganisatie om dit aan te tonen. Uit recent onderzoek blijkt dat van de organisaties die op zoek zijn naar een (nieuwe) ICT leverancier, meer dan 80% aantoonbare zekerheid wenst over de zorgvuldige werkwijze op het gebied van de opslag, verwerking en het beheer van gegevens en apparatuur.

Aantoonbare zekerheid over de betrouwbaarheid van de dienstverlening
In de praktijk blijkt dat klanten steeds vaker eigen beleid opleggen aan serviceorganisaties, variërend van één A4'tje tot zeer gedetailleerde controls.
'Algemene' certificeringen zoals de ISO-IEC 27001, schieten vaak tekort doordat zij niet specifiek genoeg zijn. Een ISAE 3402 verklaring (voorheen SAS70 genoemd) is dan de meest geschikte oplossing. Gelet op diverse contractuele verplichting jegens opdrachtgevers, kan uw organisatie zich hiermee onderscheiden van concurrenten. Een ISAE 3402 verklaring wordt steeds vaker als knock-out criterium gehanteerd bij aanbestedingen.

ISAE 3402 vervangt de SAS70 verklaring
De SAS 70-standaard is eind jaren '70 ontworpen en is om een aantal redenen vervangen. Zo ging de SAS 70-standaard niet uit van een risicobenadering, was de reikwijdte beperkt tot de betrouwbaarheid van financiële rapportages en konden shared service centers er geen gebruik van maken. Een ander belangrijk verschil is dat het management van de serviceorganisatie wordt gevraagd om een response. Deze response maakt onderdeel uit van de rapportage.

Waarom Duijnborgh Audit
Duijnborgh Audit is gespecialiseerd op het (brede) gebied van IT-auditing. Onze medewerkers zijn allen gekwalificeerde IT-auditors en door ons lidmaatschap van de NOREA (Nederlandse organisatie van Register EDP-auditor) zijn onze klanten verzekerd van een onafhankelijke beoordeling.
Wij adviseren regelmatig organisaties bij de opzet en implementatie van (ICT) beheersmaatregelen. Wij zien audits niet zozeer als 'beoordeling van…' maar meer als instrument voor organisaties om in te zetten ter verbetering van de processen. Wij streven met onze aanpak een betrouwbare en integere informatievoorziening na.

Doelstelling ISAE 3402 verklaring

Doelstelling van een International Standard on Assurance Engagements (ISAE) 3402-assurancerapport is zekerheid geven omtrent de kwaliteit van de interne beheersingsmaatregelen die verband houden met de diensten die de betreffende serviceorganisatie levert (bijv. ASP-diensten, SAAS-diensten, et cetera). ISAE 3402 kent twee typen rapporten: type 1 en 2. Een type 1 rapport betreft een onderzoek naar de opzet en het bestaan (de beschrijving en implementatie van gewenste beheersmaatregelen). Bij type 2 wordt ook de effectieve werking van de gewenste beheersmaatregelen onderzocht gedurende een bepaalde periode.

Gefaseerde aanpak

Onze aanpak is er op gericht aan uw organisatie in twee stappen de ISAE 3402 type 2 verklaring te verstrekken.

1. Start

Bij de start zullen we met uw organisatie vaststellen wat de scope dient te zijn van de audit en wat de gewenste planning is.

2. en 3. Risicoprofiel en beheersingsdoelstellingen opstellen

In deze stap brengen we samen met uw organisatie de risico's in beeld die betrekking hebben op de omgeving waarvoor u de verklaring laat opstellen. Op basis van de risico's kunnen we vervolgens gezamenlijk vaststellen wat de noodzakelijke beheersingsdoelstellingen en -maatregelen zijn.

4. Pre-audit en terugkoppeling

De beheersmaatregelen worden in opzet, bestaan en werking in een korte tijd gecontroleerd om een eerste indruk te verkrijgen. De bevindingen worden aan u teruggekoppeld. Op basis van de uitkomsten van de pre-audit wordt tevens vastgesteld wanneer stap 6 kan starten.

5. Iteratief proces verbeteracties

Op basis van de uitkomsten van de pre-audit brengt uw organisatie gewenste verbeteringen aan. Duijnborgh Audit is gedurende deze periode –en waar dat binnen haar auditrol past- beschikbaar voor het tussentijds beoordelen van de verbeteracties. Hierdoor worden verrassingen achteraf voorkomen en wordt de kans van slagen bij de eindbeoordeling aanzienlijk vergroot.

6. Audit opzet en bestaan beheersmaatregelen (SOC 2, type 1)

Op het moment dat uw organisatie aangeeft dat zij klaar is voor de 'eindaudit SOC 2, type 1' zullen wij een onderzoek uitvoeren ter beoordeling van de opzet en het bestaan. Er van uitgaande dat alle daarvoor bekende en gerapporteerde tekortkomingen zijn verholpen en dat alle noodzakelijke beheersmaatregelen zijn geïmplementeerd, wordt de audit afgerond met de afgifte van een ISAE 3402 SOC 2 rapport type 1, waarin Duijnborgh Audit een verklaring afgeeft over de getrouwheid van de beschrijving van de serviceorganisatie, de geschiktheid van het ontwerp en de implementatie van noodzakelijke beheersmaatregelen (naar de stand van dat moment).

7. Iteratief proces borging beheersmaatregelen

Gedurende een bepaalde periode (minimaal zes maanden) zorgt de auditee voor een effectieve en aantoonbare borging van de geïmplementeerde beheersmaatregelen. Evenals bij stap 5 is Duijnborgh Audit gedurende deze periode –en waar dat binnen haar auditrol past- beschikbaar voor het tussentijds beoordelen van eventuele verbeteracties.

8. Audit effectieve werking beheersmaatregelen (SOC 2, type 2)

Op het moment dat uw organisatie aangeeft dat zij klaar is voor de 'eindaudit SOC 2, type 2' zullen wij een onderzoek uitvoeren ter beoordeling van de effectieve werking van de getroffen beheersmaatregelen gedurende een bepaalde periode. De audit wordt afgerond met de afgifte van een ISAE 34032 SOC 2 rapport type 2, waarin Duijnborgh Audit een verklaring afgeeft over de getrouwheid van de beschrijving van de serviceorganisatie, de geschiktheid van het ontwerp en de effectieve implementatie van noodzakelijke beheersmaatregelen (gedurende de periode waar het onderzoek over gaat).

Duijnborgh audit b.v.
Archimedesbaan 18-H
3439 ME Nieuwegein
T 31(0)30 - 630 4108
F 31(0)30 - 630 4109
E info@dbaudit.nl

DUIJNBORGH AUDIT®