ISAE3402

U oriënteert zich op ISAE3402? Dit is wat u moet weten.

1. ISAE3402 is een internationale standaard voor auditors waarin richtlijnen zijn opgenomen voor het beoordelen van serviceorganisaties en het afgeven van een verklaring over de kwaliteit van dienstverlening. Behalve ISAE3402 bestaan er ook andere ISA-standaarden, zoals ISA3000. De ISAE3402 is op dit moment de meest populaire standaard. Alleen auditors aangesloten bij de International Federation of Accountants (IFAC) mogen een dergelijke verklaring afgeven.
2. Binnen ISAE3402 wordt onderscheid gemaakt tussen gebruikersorganisaties (klanten) en serviceorganisaties (leveranciers). Door middel van ISAE3402 geeft de serviceorganisatie aan de gebruikersorganisatie(s) inzicht in de getroffen maatregelen van interne beheersing ofwel de kwaliteit van de interne organisatie. Vaak gebruikt het management van de gebruikersorganisatie alsmede ook de accountant van de gebruikersorganisatie de ISAE3402-verklaring voor het verkrijgen van comfort (nachtrust) over de kwaliteit van dienstverlening.
3. Een ISAE3402 bestaat uit een systeembeschrijving en een verklaring van de auditor. De systeembeschrijving is een document dat onder verantwoordelijkheid van de leiding van de serviceorganisatie wordt opgesteld. De verklaring is het resultaat van het onderzoek door de auditor.
4. De systeembeschrijving moet aan bepaalde eisen voldoen en kent een vaste indeling. Behalve dat de dienstverlening en de interne organisatie dienen te worden beschreven, moeten ook beheersdoelstellingen en beheersmaatregelen zijn vastgelegd.
5. De serviceorganisatie hoeft niet ‘alle’ interne beheersmaatregelen te documenteren en moet zich beperken tot de maatregelen welke van invloed zijn op de dienstverlening aan de gebruikersorganisatie. Om dit vast te stellen moet de serviceorganisatie een risicoanalyse op de dienstverlening uitvoeren. Dit proces en het resultaat van het proces moeten worden voorgelegd aan de auditor.
6. Het uitvoeren van een risicoanalyse is een verplicht onderdeel in de totstandkoming van de ISAE3402. Deze moet worden uitgevoerd vanuit de optiek van de gebruikersorganisatie. Welke risico’s loopt de gebruikersorganisatie door afname van de dienst waardoor de gebruikersorganisatie directe of indirecte financiële schade zou kunnen leiden? En vervolgens, wat kan er bij de serviceorganisatie misgaan of gebeuren waardoor de kwaliteit van de dienstverlening kan worden verstoord?
7. De resultaten van de risicoanalyse zijn bepalend voor de in de systeembeschrijving op te nemen beheersdoelstellingen en beheersmaatregelen.
8. ISAE3402 kent twee typen verklaringen, te weten een “type I” en een “type II”. Het type houdt verband met de reikwijdte van de werkzaamheden van de auditor. Bij een type I beoordeelt de auditor de opzet en het bestaan van de beheersmaatregelen; in de Engelse literatuur wordt dit ‘design effectiveness’ genoemd. Bij een type II beoordeelt de auditor de werking van de beheersmaatregelen over een langere periode. In de Engelse literatuur wordt dit ‘operational effectiveness’ genoemd. Een type I en type II verhouden zich als de foto (momentopname) en de film (waarnemingen over een langere periode). Voor een type II-onderzoek moet de auditor de werking van de maatregelen over een periode van minimaal 6 maanden onderzoeken. Doorgaans wordt voor een periode van 1 jaar gekozen en loopt deze periode gelijk met het financiële boekjaar van de onderneming. Indien de rapportage ten behoeve van de jaarrekeningcontroles van gebruikersorganisaties wordt opgesteld, wordt er jaarlijks een nieuw type II-rapport opgesteld.
9. Het onderzoek van de auditor stelt eisen aan de manier waarop de serviceorganisatie de opzet van de maatregelen documenteert, de manier waarop de serviceorganisatie de maatregelen aantoonbaar uitvoert en de manier waarop het management toezicht houdt op de naleving van de uitvoering. Immers, achteraf dient de auditor te kunnen vaststellen dat de organisatie zich aan de eigen regels heeft gehouden. Met name op het opstellen van de maatregelen en het zorgen dat er een voldoende audittrail wordt opgebouwd, kost de nodige interne inspanning.
10. SSAE16 is net als ISAE3402 een standaard om serviceorganisaties te beoordelen. SSAE16 is een standaard van de Amerikaanse accountantsorganisatie. De twee standaarden komen in grote lijnen met elkaar overeen, maar er zijn ook belangrijke verschillen. SSAE16 onderscheidt ook een type I en een type II, maar daarnaast kent SSAE16 ook onderscheid naar SOC 1, SOC 2 en SOC 3. Soms wordt deze indeling ook voor ISAE3402 gebruikt. Deze indeling heeft betrekking op de scope en het normenkader van de systeembeschrijving. SOC 1 is ten behoeve van de jaarrekeningcontroles van gebruikersorganisaties en heeft een vrij kader. SOC 2 is met name bedoeld voor IT-outsourcing en bestaat uit een vaste kader van maatregelen. SOC 3 betreft een publicatievariant op SOC 2.

ISAE3402

Wat moet u doen?

Wat u als serviceorganisatie moet doen om voor ISAE3402 in aanmerking te komen verschilt sterk per organisatie en hangt af van het huidige volwassenheidsniveau, de ambities van de organisaties en herbruikbaarheid vanuit reeds beschikbare keurmerken. Onderstaand vindt u een overzicht van de stappen die iedere organisatie moet doorlopen en op welke manier daar invulling aangegeven kan worden. De inspanning kan dus verschillen, maar deze kunnen wij in overleg met u bepalen.

1 Begin bij het vaststellen van de scope: Voorafgaand aan het project is het essentieel dat de dienstverlening aan de gebruikersorganisaties eenduidig beschreven is en dat ook directe en indirecte financiële risico's voor de gebruikersorganisatie gedocumenteerd zijn.

2 Identificeer risico's en definieer beheersdoelstellingen: Voer een risicoanalyse op de kwaliteit van de interne organisatie uit en identificeer mogelijke gebeurtenissen die gevolgen kunnen hebben voor de kwaliteit van dienstverlening en in het bijzonder hetgeen financiële risico's kan veroorzaken. Bijvoorbeeld fouten, vergissingen, verstoringen, fraude, sabotage, overmacht. Schrijf de risico's zo concreet mogelijk op. Dit helpt om straks beter de maatregelen te kunnen uitwerken. Gebruik de uitkomsten van de risicoanalyse om te bepalen welke aspecten, onderdelen en processen van de interne organisatie aandacht behoeven en formuleer dit in beheersdoelstellingen.

3 Uitwerken van het beheerskader: Bij ISAE3402 gaat het erom dat de serviceorganisatie voldoende maatregelen heeft getroffen om de beheersdoelstellingen te waarborgen. De set aan maatregelen garandeert dat de doelstellingen worden bereikt. Deze stap gaat over het bepalen van de set aan maatregelen. Veel organisaties beginnen hiermee door de huidige maatregelen te inventariseren en te onderzoeken of er voldoende maatregelen zijn getroffen om altijd alle risico's tijdig te signaleren en weg te nemen. Uiteindelijk volgt hieruit een analyse van maatregelen die er al wel zijn en maatregelen die nog moeten worden getroffen. Alleen belangrijkste maatregelen vormen samen het beheerskader.

4 Documenteren en implementeren: Met het uitwerken van het beheerskader in stap 3 is een belangrijke mijlpaal gerealiseerd. Er is namelijk bekend wat de scope van de ISAE3402 wordt. Het is vanaf hier vooral een kwestie van documenteren, implementeren en bewaken. Het is onze ervaring dat deze stap wel de meeste tijd en inspanning vergt. Alle maatregelen moeten in opzet worden beschreven in bijvoorbeeld beleidsdocumenten, procedures, procesbeschrijvingen en werkinstructies. Afhankelijk van de hoeveelheid aan maatregelen en reeds beschikbare opzetdocumentatie is dit nauwelijks of juist heel veel werk. ISAE3402 stelt daarbij ook eisen aan de opzet documentatie. Dus daarop moet worden gecontroleerd. Systemen en medewerkers van de organisatie moeten worden voorbereid op de nieuwe set van maatregelen. De uitvoering van de maatregelen moet aantoonbaar zijn hetgeen tot uitdrukking moet worden gebracht in een audittrail. Medewerkers moeten worden geïnstrueerd en worden begeleid.

5 Bewaken van de uitvoering: Na implementatie van de maatregelen in de organisatie moet worden gezorgd dat de maatregelen ook standhouden en dat een en ander wordt uitgevoerd conform de opzet. Als de bewaking hierop ontbreekt kan het voorkomen dat de auditor straks constateert dat maatregelen onvoldoende aanwezig zijn. Veel organisaties stellen dan ook een interne monitoringfunctie aan, bijvoorbeeld als onderdeel van kwaliteitszorg of in de vorm van periodieke rapportages aan het management.

6 Opstellen van de systeembeschrijving: Het schrijven van de systeembeschrijving kan feitelijk al worden gestart zodra het beheerskader bekend is (zie stap 3). Er zijn diverse templates beschikbaar die u kunnen helpen in het opstellen van de systeembeschrijving. Onze ervaring is dat de meeste informatie reeds in uw organisatie voorhanden is.

7 De audits: Als de systeembeschrijving klaar is, alle beheersmaatregelen zijn geïmplementeerd en de maatregelen minimaal één keer zijn uitgevoerd dan kan een auditor een type I-onderzoek uitvoeren. De auditor zal de systeembeschrijving nodig hebben om de kosten van zo'n onderzoek te kunnen inschatten. Met name het aantal te controleren beheersdoelstellingen en het aantal te testen beheersmaatregelen bepalen de kosten van zo'n onderzoek. Na een minimale periode van 6 maanden kan een auditor een type II-onderzoek uitvoeren.

Nog vragen? **ControlSolutions International** is u graag van dienst. Bel 020-658 6175 of mail naar netherlands@controlsolutions.com